Journal of Healthcare Engineering

Securing the Internet of Health Things (IoHT) with Lightweight Security Schemes

Lead Guest Editor: Muhammad Asghar Khan
Guest Editors: Mohammed H. Alsharif and Azeem Irshad

Securing the Internet of Health Things (IoHT) with Lightweight Security Schemes

Journal of Healthcare Engineering

Securing the Internet of Health Things (IoHT) with Lightweight Security Schemes

Lead Guest Editor: Muhammad Asghar Khan
Guest Editors: Mohammed H. Alsharif and Azeem Irshad

Associate Editors

Academic Editors

Contents

Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 1177635, 13 pages
https://doi.org/10.1155/2023/1177635

Research Article

Learning to Discriminate Adversarial Examples by Sensitivity Inconsistency in IoHT Systems

Huan Zhang,[1,2] **Hao Tan,**[1,2] **Bin Zhu,**[1] **Le Wang,**[1] **Muhammad Shafiq,**[1] **and Zhaoquan Gu**[2,3]

[1]*Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China*
[2]*Department of New Networks, Peng Cheng Laboratory, Shenzhen, China*
[3]*School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen, China*

Correspondence should be addressed to Muhammad Shafiq; srsshafiq@gmail.com and Zhaoquan Gu; guzhq@pcl.ac.cn

Received 21 June 2022; Revised 12 August 2022; Accepted 24 November 2022; Published 22 February 2023

Academic Editor: Muhammad Asghar Khan

Deep neural networks (DNNs) have been widely adopted in many fields, and they greatly promote the Internet of Health Things (IoHT) systems by mining health-related information. However, recent studies have shown the serious threat to DNN-based systems posed by adversarial attacks, which has raised widespread concerns. Attackers maliciously craft adversarial examples (AEs) and blend them into the normal examples (NEs) to fool the DNN models, which seriously affects the analysis results of the IoHT systems. Text data is a common form in such systems, such as the patients' medical records and prescriptions, and we study the security concerns of the DNNs for textural analysis. As identifying and correcting AEs in discrete textual representations is extremely challenging, the available detection techniques are still limited in performance and generalizability, especially in IoHT systems. In this paper, we propose an efficient and structure-free adversarial detection method, which detects AEs even in attack-unknown and model-agnostic circumstances. We reveal that sensitivity inconsistency prevails between AEs and NEs, leading them to react differently when important words in the text are perturbed. This discovery motivates us to design an adversarial detector based on adversarial features, which are extracted based on sensitivity inconsistency. Since the proposed detector is structure-free, it can be directly deployed in off-the-shelf applications without modifying the target models. Compared to the state-of-the-art detection methods, our proposed method improves adversarial detection performance, with an adversarial recall of up to 99.7% and an $F1$-score of up to 97.8%. In addition, extensive experiments have shown that our method achieves superior generalizability as it can be generalized across different attackers, models, and tasks.

1. Introduction

Recently, the fast development of deep neural networks (DNNs) has resulted in DNN-based models being applied in many scenarios around the Internet of Things, such as smart transportation [1, 2], intelligence healthcare [3], social networks [4], and information encryption [5, 6]. At the same time, the rapid proliferation of attacks against DNN-based models has raised greater security concerns [7]. Among them, adversarial attacks, which are novel and powerful, have caused harmful effects on model performance. In this paper, we study the security problems of the Internet of Health Things (IoHT) systems against adversarial attacks. As text data is a commonly adopted form in IoHT systems, such as the patients' basic information, medical records, and prescriptions, we focus on the security problems that may exist in such DNN-based textual analysis models.

As textual adversarial attacks exist in various forms and implement discrete perturbations, it has been a tough challenge to defend against such attacks in the DNN-based IoHT systems. Some defense methods against adversarial attacks have been proposed to address this challenge. The current approaches mainly focus on adversarial training [8, 9] and adversarial data augmentation [10, 11], which typically require retraining target models and extensive prior knowledge of attacks. Another type of defense method is input reconstruction [12, 13], which can be directly deployed into unmodified target models but hurts accuracy. In contrast, adversarial detection is a more direct defensive strategy that only detects adversarial examples (AEs) without correcting them [14–16]. In practical applications, this strategy has a high value because it alerts to threatening inputs and then rejects or submits them to other processing, rather than expecting the target model to give ambiguous and unreliable outputs. Obviously, adversarial detection is more appropriate in IoHT systems due to the hardware constraints. Unfortunately, very little attention has been paid to detection, and the available detection techniques are still limited in performance and generalizability.

In this work, we focus on adversarial detection. The goal of this study is to improve detection performance and generalizability. Based on sensitivity inconsistency to perturbation, we employ adversarial features, which are extracted from the shift of predicting labels and the similarity of probability distributions, to train a detector. The proposed method is efficient and high-transferable, which can catch AEs even in the circumstances of attack-unknown and model-agnostic.

We understand the difference between AEs and normal examples (NEs) in terms of geometric translation. An adversarial example can be regarded as a normal example changing along the adversarial direction. Geometrically, the adversarial direction usually points to the region where the decision boundary is highly curved [17]. Meanwhile, a study has pointed out that AEs easily lead to different classifications if fluctuations are caused at highly curved regions in the image domain [18]. Considering the goal of the attack, the adversarial examples are distributed centrally around the decision boundary to ensure low modification and imperceptibility. Thereby, we point to a common phenomenon: the AEs are boundary-sensitive. If we perturb the sensitive part of the AEs, it is extremely easy to cross the decision boundary. We consider important words (IWs) that contribute significantly to the decision as sensitive parts. As shown in Figure 1, if we intentionally perturb the IWs in examples, AEs easily lead to the target model making different predictions, while NEs maintain consistent behavior with the original.

To confirm this conjecture, we perturb the most important word in a set of AEs and NEs separately and illustrate the change in predictions of the model in Figure 2. As the result shows, in the NEs, perturbation of the most significant word leads to a shift in the probability values, but none crosses the decision boundary. However, in AEs, the same perturbation leads to prediction label changes in most examples. Further, the results show that even though the predicting labels of NEs change, the probability is closer to the decision threshold. It indicates that in NEs, the probability distributions in the Softmax layer are much closer before and after IWs are perturbed than those in AEs.

This preliminary work inspired us to design a detector trained with adversarial features that are extracted from perturbation-sensitive inconsistencies between NEs and AEs. We conclude that the sensitive inconsistency between NEs and AEs manifests in two parts: (1) whether the predicting label is changed after perturbing IWs; and (2) the inconsistency of the degree of change in probability distributions before and after perturbation. We combine the two points of sensitive inconsistency as the final adversarial feature. Our major contributions can be summarized as follows:

(1) We propose an adversarial feature extraction method, named Sensitive Inconsistency Feature (SIF). As SIF is obtained from the universal differences between NEs and AEs, it can be generalized to different attack scenarios, even if they have never been known before.

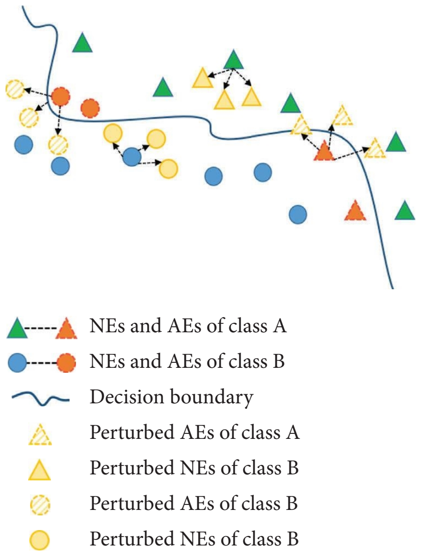


Figure1: A visual illustrative example for sensitivity inconsistency of NEs and AEs against perturbing important words (IWs). The black arrow points to the direction of example movement (relative to the decision boundary) after IWs are perturbed. The figure shows that the perturbed AEs cross the decision boundary with high probability, but the NEs do not.

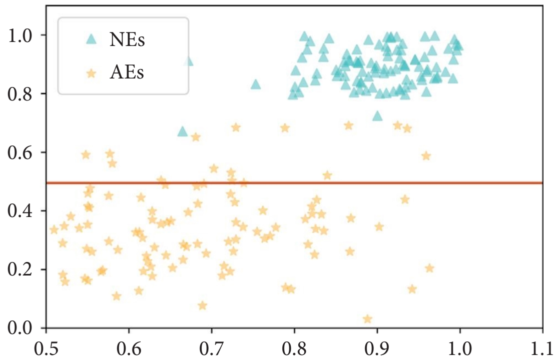


Figure 2: Visualization of probabilities values of NEs and AEs to the predicting label before perturbation. The AEs are generated by TextFooler attacking the CNN-based model. The x-axis and y-axis indicate the probability values for the true label before and after perturbation. Since the red line is $y = 0.5$ and the IMDB dataset is a binary classification, the elements below the red line are examples that the predicting label changes.

(2) We implement the adversarial detection method using SIF and machine learning mechanisms, named SIF Detector (SIFD). The experiments show our detection recall rate is up to a maximum of 99.7%, and the $F1$-score is 97.8% on IMDB, demonstrating its superiority over current advanced methods.

(3) We present that SIFD exhibits transferability capabilities. In the most challenging settings (i.e., all of the configurations in the learning and detection phases are inconsistent), the $F1$-score and recall rates remain above 85%. All the codes to reproduce our experimental results are open source at https://github.com/AuroraHuan/SIFD-adversrial-detection and we hope they facilitate future research.

The remainder of this paper is organized as follows: Section 2 reviews the existing studies on adversarial attacks and defenses. Section 3 describes the proposed detection method, SIFD. Experimental details, results, and analysis are given in Section 4. Finally, in-depth discussions and conclusions are given in Sections 5 and 6.

2. Related Work

This section briefly reviews adversarial attacks and defenses. As a hot research topic in recent years, there has been a lot of work on adversarial attacks. We focus on word-substitution attacks, which have received more attention as they perform better in semantic preservation and semantic correctness. Compared to other categories of attacks, word-substitution attacks better balance aggressiveness and concealability. As mentioned in the first section, we divide adversarial defenses into three categories, and in this section, we pay particular attention to adversarial detection, which is most relevant to our study.

2.1. Adversarial Attack. Given a text x, the attacker adds imperceptible perturbation δ to x to generate the adversarial example $x_{adv} = x + \delta$ and aims to make the pre-trained model F misclassify, where the perturbation includes adding, deleting, and replacing characters or words.

2.1.1. Gradient-Based Attack. As images are encoded as numerical vectors, perturbations generated by gradient sign methods are easily transformed into corresponding images [19–22]. However, these methods are not compatible with the textual domain because of the natural discreteness of texts. Therefore, for NLP tasks, gradient-based methods are usually combined with heuristic algorithms to generate adversarial examples, including the utilization of the value of the gradient to determine important words [23], sentences [24], or the ranking of perturbed substitutions [20, 25].

2.1.2. Confidence-Based Attack. In this category, the attacker can obtain the classification confidence of each label. A common attack process includes two steps: (1) score the words according to confidence and sort them in descending order; and (2) sequentially perturb the sorted words until the attack succeeds or stops when it reaches the perturbation limit. The greedy search strategy is widely used to find optimal replacements in confidence-based attacks [10, 11, 26–28]. Besides, the genetic algorithm and bean search are also common search strategies [29, 30].

2.1.3. Decision-Based Attack. The most challenging attack scenario is when the attackers only have access to the predicted labels of the target model. In this case, the attackers usually generate a weak adversarial example, followed by optimizing it until it generates a strong AE that is most similar to the original text [31, 32].

2.2. Adversarial Defense

2.2.1. Robustness Enhancement. Gradient-based adversarial training is widely used for defense in the vision field [19, 21] with satisfactory effects, while in the natural language field it is effective in improving the accuracy and generalization of models [8, 33] but has weak gains in adversarial robustness. As a result, virtual adversarial training is widely used for textual adversarial robustness [9, 34, 35]. In addition, adversarial data augmentation [10, 27, 36] and virtual adversarial data augmentation [37] also effectively improve the adversarial robustness of models, but such methods are prone to decrease model accuracy. Zhu et al. [38] proposed a combination of friendly data augmentation and gradient-based adversarial training that can improve the adversarial robustness of models while maintaining their accuracy.

2.2.2. Input Reconstruction. Discrete text is transformed into embedding vectors before input to the model, so many defense methods utilize reencoding to defend against spelling error attacks [36] and synonym attacks [39]. In addition, text-level reconstruction methods [12, 13] have been used to defend against word-substitution attacks. Among them, except for the method proposed in [13], the rest of the methods are effective for specific attacks and are not generalizable.

2.2.3. Adversarial Detection. Different from the two types of defense methods mentioned above, adversarial detection only reports anomalies without correcting them. Although detections have been well used in the image domain [17, 40, 41], there are scarce studies on textual adversarial learning. Zhou et al. [14] trained a perturbation detector to detect potential perturbations and an embedding estimator to restore perturbations based on the BERT model [42], but trained by special AEs makes it difficult to generalize and the training of the BERT model is time-consuming. Mozes et al. [15] proposed detecting AEs through a simple and effective feature-word frequency, but this approach is only applicable to word-level attacks. Mosca et al. [16] trained a logit-based adversarial detector and achieved the best detection results in text classification so far.

3. Method

3.1. Overview of SIFD. Focusing on adversarial detection, the core of our idea is to extract distinguishable adversarial features and train a detector based on these features, and the overall process is shown in Figure 3. The intuition behind the approach is that even though AEs and NEs are extremely similar in semantics and visuals, they react inconsistently when important words are perturbed, i.e., the target model differs dramatically in output changes for AEs and NEs. The proposed method is divided into three steps: first, we inspect whether the predicting label has changed and mark it as a label inconsistency ($S(x, f)$ in Figure 3); then we calculate the similarity of the probability distribution of the Softmax layer ($J(x, f)$ in Figure 3); last, we combine features and train a detector.

3.2. The Feature of Sensitivity Inconsistency. For a given input text $x = w_1, w_2, \ldots, w_n$, including n words and the target model F, the process for extracting features is shown in Algorithm 1, including three main steps:

(1) Ranking words and extracting IWs. We design an importance scoring function to rank the words in the text and select a specified number of IWs to participate in subsequent feature extraction.

(2) Marking the word sensitivity signals. We define the concept of sensitive words for IWs and assign different values to sensitive and nonsensitive words.

(3) Calculating the similarity of the probabilities distribution before and after perturbing IWs. Detailed explanations of the three steps are given in Subsection 3.2.1, 3.2.2, and 3.2.3, respectively.

3.2.1. Ranking Word Importance. For attackers, regardless of the variations in the means of generating AEs, the ultimate goals are the same: minimizing the modification rate and maximizing the semantic similarity between AEs and their corresponding NEs, which are defined as the basic conditions of satisfying the adversarial example. To achieve these goals, attackers usually pick important words and perturb them, rather than make meaningless modifications to some unimportant words. Therefore, important words are powerful signals of the difference between the AEs and NEs, which consequently become the most critical features for adversarial detection.

Important words contribute much to the predicting of F so that the prediction probability changes significantly after removing it from x. We denote the contribution of a word w_i to x in model F by $I(w_i, x, f)$ which is usually expressed as

$$I(w_i, x, f) = \begin{cases} \left(x_{\backslash w_i}, y_i\right) - f(x, y_i) + f(x, y) - f\left(x_{\backslash w_i}, y\right), & f \text{ if } y_i \neq y, \\ f\left(x, y_j\right) - f\left(x_{\backslash w_i}, y_j\right), & \text{others,} \end{cases} \tag{1}$$

where $x_{\backslash w_i}$ is text x that removes w_i, $f(x, y_j)$ is the probability value of x to class y_j, y is the predicting class of x according target model F, and y_i is the predicting class of $x_{\backslash w_i}$.

However, for a long text which consists of multiple sentences, this processing is time-consuming as it requires n forward calculation on F, where n is large. Our goal is to improve the efficiency of the processing. Following the study in [19, 23], we use the gradient magnitude to estimate the contribution of each word to prediction. The direction of gradient descent is the optimization signal to assist the model to obtain the minimum loss in the training phase; therefore, the word whose direction is close to the gradient contributes much to predicting F. According to this, we measure the importance of words by only 1 inquiry to F. Specifically, we utilize dot product to represent the angle between w_i and gradient on w_i, which is calculated as

$$I(w_i, x, f) = V_{w_i} \bullet \nabla_{w_i} J(\theta, x, f(x)), \tag{2}$$

where V_{w_i} is the embedding of w_i, v is the embedding dimension, and J is the loss function of F.

After ranking all words in x by equation (2), we further filter stop words from NLTK (https://ww.nltk.org/) and SpaCy (https://spcay.io/) libraries. Furthermore, we use NLTK to filter parts of speech, keeping only verbs, adverbs, adjectives, nouns, and their derived expressions, which correspond to the 16 lexical properties in NLTK. Finally, we select the most important k words as the feature source of text x for subsequent feature extraction, which is denoted as $C(x)$.

3.2.2. Marking Sensitivity Signals. AEs and NEs respond differently to the perturbing IWs. The predicting labels of AEs are highly susceptible to change due to the boundary sensitivity of AEs. In contrast, the probabilities for NEs in each class change, but the final predicting label remains relatively stable, which is similar to the principle of partial distortion of images without affecting the decision of the model [40]. Based on reaction inconsistency, we propose a method to define the sensitivity of the input x: for each word in $C(x)$, we obtain the prediction classes before and after the word is removed, and then we define the word with different prediction classes as the sensitive word, and vice versa as a nonsensitive word. More precisely, the removal operation indicates the replacement of the original word as <MASK> for the pretrained models such as BERT and RoBERTa and <unk> for the traditional DNNs model such as LSTM and CNN. Furthermore, the set of signals based on sensitive words is adopted as the measure of the text sensitivity to F, denoted as $S(x, f)$, which is formalized as

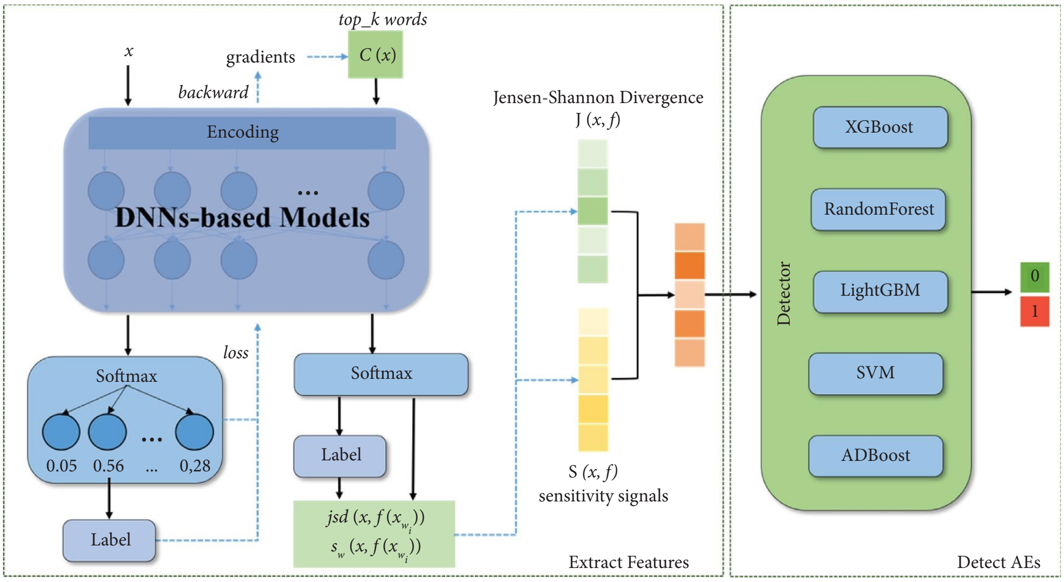


Figure 3: The workflow of the proposed detection method SIFD.

```
Input: Text $x$, target model $f$
Output: Feature matrix $E$
Initialization: feature matrix $E \longleftarrow [0]$, scores of words $S \leftarrow$ None
Get the predicting label $y \longleftarrow f(x)$
$S[w_i] \longleftarrow V_{w_i} * \nabla_{w_i} J(\theta, x, f(x))$ for each valid $w_i$ in $x$
$S \longleftarrow$ sort $S$
$C(x) \longleftarrow$ most important $k$ words according $S$
for each $w$ in $S$ do
    $j \longleftarrow jsd(f_s(x), f_s(x_{\backslash w_i}))$ by (5)
    if $f(x) = f(x_{\backslash w_i})$ then
        $s \longleftarrow 1$
    else
        $s \longleftarrow -1$
    end if
    add $j * s$ to $E$
end for
```

Algorithm 1: Feature extraction based on sensitivity inconsistency.

$$S(x, f) = \left\{ s_w\left(x, x_{\backslash w_i}, f\right) \right\} \; s.t. \; w_i \in C(x), \tag{3}$$

where $s_w(x, x_{\backslash w_i}, f)$ is a word-sensitive signal that is calculated as

$$s_w\left(x, x_{\backslash w_i}, f\right) = \begin{cases} 1, & \text{if } f(x) = f\left(x_{\backslash w_i}\right), \\ -1, & \text{if } f(x) \neq f\left(x_{\backslash w_i}\right). \end{cases} \tag{4}$$

3.2.3. Distribution Difference of Softmax Layer. It is not enough to rely on sensitivity signals alone to distinguish AEs and Nes, as discrete signals make it easy to cause many NEs to be incorrectly recalled as AEs. Furthermore, this error is more explicit in short-length texts because IWs in NEs are sensitive to perturbation. To solve this problem, we employ the inconsistency of the changes in probability distribution (i.e., the confidence scores of x predicted by F to all classes) of the Softmax layer as another feature. It signifies a more nuanced difference between AEs and NEs. Therefore, we use the Jensen-Shannon Divergence (JSD) to calculate this feature, which is expressed as

$$jsd\left(x, x_{\backslash w_i}, f\right) = \frac{1}{2} \mathrm{KL}\left(f_s(x) \| M\right) + \frac{1}{2} \mathrm{KL}\left(f_s\left(x_{\backslash w_i}\right) \| M\right), \tag{5}$$

where $f_s(x)$ is the Softmax output, and $M = (1/2)(f_s(x) + f_s(x_{\backslash w_i})$ and KL is the Kullback–Leibler divergence, for which the formula is

$$KL(p\|q) = \sum p(x)\log\frac{p(x)}{q(x)}. \quad (6)$$

For each word in $C(x)$, we calculate the JSD values according to equation (5) and use these values as the distribution variance features of x, denoted as

$$J(x, f) = \left\{jsd\left(x, x_{\backslash w_i}, f\right)\right\} s.t.\ w_i \in C(x). \quad (7)$$

3.3. Training Detector

3.3.1. Extracting of Distinguishable Features. The final input feature is calculated by combining the sensitivity flags $S(x, f)$ and JSD values $J(x, f)$

$$E(x, f) = S(x, f) * J(x, f). \quad (8)$$

Thus, the input features for the adversarial detector are a set of continuum vectors of size *k*, and the labels are binary, 0 for NEs and 1 for AEs. In the training phase, we divide the data into a training set and a test set in the ratio of 8 : 2. In the test phase, the input features are computed by querying the target model $k + 1$ times. Compared to the work in [16], which requires *n* queries, we save time costs in feature extraction and consider more distinguishable features. In Subsection 5.2, the advantages of combined features are demonstrated by ablation experiments.

3.3.2. Design of the Detector. Following Mosca et al. [16], we do not fix detector architecture, and we train multiple machine learning models and evaluate their effects. Notably, our method does not depend on a specific model or a specific classification task, i.e., the detector can be deployed as a plug-and-play add-on to the target model to improve robustness. Moreover, although our detection method depends on the adversarial corpus, it is not limited to a specific attack method because the adversarial feature extraction method we design is based on the generic characteristics of AEs. Our proposed adversarial detection method is generalizable, which manifests in model agnostic, attack transportability, and data compatibility. In Subsection 4.4, we conduct an all-around analysis of the generalizability of our proposed method.

4. Experiments

4.1. Experiment Setup

4.1.1. Datasets and Tasks. We adopt three popular classification benchmark datasets for our experiments: Internet movie reviews from IMDB [43], news articles on the web from AG's news [44], and the Yelp dataset challenge with polarity label [44]. As all of them are without a standard split for train/dev/test, we divide the original training set into training set and development set in a ratio of approximately 9 : 1. The statistics of them are shown in Table 1.

4.1.2. Models. We adopt four DNN models that achieve state-of-the-art performance on text classification: BERT [42], RoBERTa [45], CNN [46], and LSTM [47]. Specifically, we use the pretrained BERT model and RoBERTa model with 12 transformer layers, 12 self-attention heads, and a hidden size of 768. We set dropout as 0.1 and epochs as 10, and fine-tune them with a batch size of 64 for AG's news and 32 for the others. The CNN model contains three convolutional layers with filter sizes of 3, 4, and 5. The LSTM model has 1 bidirectional layer and 128 hidden units. The inputs are initialized as embeddings by 300-dimensional pretrained word embeddings Glove [48] (https://github.com/stanfordnlp/GloVe) in LSTM and CNN. And the batch size is 256, the number of epochs is 20, and the dropout rate is 0.1 for both CNN and LSTM.

4.1.3. Attack Methods. We employ four well-established attack methods: PWWS [26], TextFooler [10, 28], and BAE [27]. PWWS and TextFooler are the strong baselines for natural language attacks based on the black-box set and generate perturbation with synonym replacement; Deepwordbug crafts visual-similarity adversarial examples with a little number of typos; and BAE generates more semantic natural AEs by using the BERT masked language model. To ensure the consistency of attacks, we set the important parameters following the study in [8, 38]. The word modification rate is 0.2 for AG's news and 0.1 for the others, depending on the text length of the different datasets, and the threshold of the minimum similarity between AEs and NEs is 0.84 to ensure the reasonableness of AEs.

4.1.4. Detection Baseline. We compare our proposed method SIFD with two other state-of-the-art detection methods FGWS [15] and WDR [16] under different combinational settings of datasets, models, and attacks. For FGWS, we follow all the detection settings of the original paper and determine the key parameter, threshold γ, which is the minimum value of the confidence difference for AE identification. For the IMDB dataset, we use the default threshold of 0.9 in the source code (https://github.com/maximilianmozes/fgws); for AG's news, referring to the tuning method and criteria in the original paper, we select $\gamma = 0.85$ with the best true positive rate under the premise that no more than 10% of NEs are judged as AEs. Given that both our method and WRD are detector-based, we used a process similar to SIFD to train and test WRD. The architecture of the WRD detector is XGBoost [49], and the parameter settings are the same as those in the original paper.

4.1.5. Evaluation Criteria. We employ several performance criteria to evaluate detection. We treat the AEs as positive examples (P) and the NEs as negative examples (N) for detection. Hence, TP denotes the number of P predicted as P, FP denotes the number of N predicted as P, TN denotes the number of N predicted as N, and FN denotes the number of P predicted as N. The criteria utilized in the experiment are as follows:

Table 1: Summary for datasets. #train, #dev, and #test count the number of texts in the train/dev/test set, respectively, #avg length is the average length of all the texts for each dataset, and #classes is the number of classes.

Dataset	#train	#dev	#test	#avg length	#classes	Task
IMDB	23,000	2,000	25,000	268	2	Sentiment analysis
AG's news	1,08,000	12,000	7,600	43	4	News classification
Yelp	5,00,000	60,000	38,000	152	2	Online reviews

$$\begin{aligned}\text{Recall} &= \frac{TP}{TP+FN},\\ \text{Accuracy} &= \frac{TP+TN}{TP+TN+FP+FN},\\ F1-\text{score} &= \frac{2*\text{Precision}*\text{Recall}}{\text{Precision}+\text{Recall}},\\ \text{Precision} &= \frac{TP}{TP+FP}.\end{aligned} \tag{9}$$

4.2. Detector Architecture Selection. We utilize multiple machine learning models as candidate architectures for the detector and compare their performances to select the model with the optimal detection performance for subsequent experiments. Specifically, we use BERT as the target model and fine-tune it on IMDB and AG's news, and then 1,500 adversarial examples generated by TextFooler for IMDB and PWWS for AG's news, separately. We extracted features from these AEs and their corresponding NEs, then divided the training, validation set, and test sets in proportions 8 : 1 : 1. Finally, we train and test five classifier models, including Random Forest [50], XGBoost [49], LightGBM [51], SVM [52], and AdaBoost [53].

As shown in Table 2, all the models achieve competitive detection performance, provided that all settings are identical. Among them, XGBoost performs slightly better, so we choose it as the detector architecture in the subsequent experiments. The main parameters of XGBoost include: the maximum depth is 3, the learning rate is 0.2, the gamma is 0.6, and other settings are disclosed in our open source code.

4.3. Detection Performance Comparison and Analysis. We compare SIFD with two advanced detection technologies. More specifically, we train and test the detectors in the same process as in Subsection 4.2, and for the nontrained FGWS, we test their performance in the tuned parameter settings. Although random sampling causes different examples to be selected each time, three detection methods compare their performance on the same examples in each configuration. As Deepwordbug is a character-level attack and FGWS detection is just designed for word-level attacks, we do not perform FGWS to detect adversarial examples generated by Deepwordbug.

As Table 3 presents, our proposed method outperforms the baseline method in 21 configurations (24 configurations in total). Even in the worse 3 configurations, the effect of our method is close to the optimal method. In addition, we observe that the effects of all detection methods on IMDB always outperform those on AG's news. To further clarify the causes of this phenomenon, we conduct a more detailed analysis in Subsection 5.3.

4.4. Transferability Evaluation. The transferability of the detector is a very important metric, as the data and models in the real-world defense phase are unpredictable and highly likely to be inconsistent with them in the training phase. In this subsection, unlike Subsections 4.2 and 4.3, we randomly sample 1000 texts (500 AEs and 500 NEs) to test the detection capability of the model for each configuration.

We first test the transferability of the detector on various attacks. Specifically, we first train the detector with the AEs generated by one attack and then test its ability to detect the AEs generated by other attacks. The detection effects with identical settings in the training and testing phases are seen as the baseline, which is called the default effect, and correspond to the row where the "*" sign is located in Table 4.

As we can see from Table 4, our method always performs well in the migration from one attack to another. Both F1-score and adversarial recall rates differ from the default effect by a maximum of no more than 3%, and are always around ± 1% and even sometimes better than the default effect.

Additionally, we test the transferability of different models. As shown in Table 5, LSTM and BERT exhibit remarkable transferability for each other, but the performance of CNN is relatively weak. We give a possible explanation for this phenomenon. We conjecture that the decision boundary of the trained CNN is more curved, and the convex region is steeper compared to the other two models. Therefore, the probability distributions vary greatly from AEs to their corresponding NEs. Therefore, the detectors learn features from these AEs that are significantly distinguishable and obtain excellent detection performance, but they struggle to detect more challenging AEs generated by other models. In addition, we observe that the attack success rate of various attack methods against the CNN model is higher than the others, and the adversarial recall ratio of detectors based on CNN is higher, which is consistent with our conjecture.

Furthermore, we consider the most challenging situation to be one in which all settings in the detection phase are different from those in the training phase. We select the detector trained by IMDB + BERT + TextFooler from Subsection 4.3 as the baseline detector and test it in two datasets, two models, and three attack methods. We trained the detector with IMDB + BERT + TextFooler and tested its detection performance with inconsistent datasets, models, and attack methods; the results are shown to the left of the parentheses in Table 6. As Table 6 shows, the scores for the two metrics are above 85% for various combinations of settings. It

Table 2: Detection performance of different machine learning model architectures. Bold values indicate the optimal results.

Dataset	Machine learning model	Accuracy (%)	Recall (%)	$F1$-score (%)
IMDB	Random forest	95.7	96.0	95.1
	XGBoost	96.1	**97.2**	**96.4**
	LightGBM	**96.3**	94.1	95.8
	SVM	92.3	93.2	92.1
	AdaBoost	95.2	96.0	94.9
AG's news	Random forest	89.5	88.1	89.0
	XGBoost	**92.7**	**91.9**	**92.2**
	LightGBM	91.7	80.4	91.3
	SVM	90.4	90.0	89.1
	AdaBoost	88.8	88.9	88.8

Table 3: Detection performance of three detection methods. The model, dataset, and attack method are consistent for the training and testing phases. As Deepwordbug is a character-level attack and FGWS detection is just designed for word-level attacks, the experimental results of Deepwordbug detection with FGWS are not meaningful, and "—" in the table indicates that the experiment is not conducted.

Model	Dataset	Attack	Recall (%)			$F1$-score (%)		
			FGWS	WDR	SIFD	FGWS	WDR	SIFD
BERT	AG's news	TextFooler	81.5	83.0	**91.7**	87.5	86.1	**90.7**
		PWWS	85.1	87.9	**91.9**	89.7	90.5	**92.2**
		BAE	49.7	80.0	**86.7**	57.2	81.2	**84.5**
		Deepwordbug	—	75.4	**85.0**	—	78.3	**85.6**
	IMDB	TextFooler	79.9	95.5	**97.2**	86.6	95.8	**96.4**
		PWWS	82.5	92.7	**95.5**	85.8	94.2	**96.0**
		BAE	56.7	90.3	**96.2**	67.8	93.1	**96.3**
		Deepwordbug	—	92.0	**94.2**	—	92.7	**94.8**
CNN	AG's news	TextFooler	82.9	92.0	**95.5**	86.2	89.7	**91.5**
		PWWS	86.8	91.0	**94.0**	91.2	86.0	**90.6**
		BAE	56.7	88.2	**92.4**	62.1	85.5	**88.5**
		Deepwordbug	—	91.0	**92.4**	—	**86.3**	84.9
	IMDB	TextFooler	75.9	89.9	**99.7**	85.3	91.5	**97.8**
		PWWS	80.2	87.2	**99.0**	86.0	87.2	**96.5**
		BAE	59.8	88.9	98.2	70.1	87.1	96.5
		Deepwordbug	—	91.2	**97.9**	—	89.6	**95.7**
LSTM	AG's news	TextFooler	86.2	91.3	**96.2**	90.1	87.8	**91.2**
		PWWS	84.7	84.6	**94.5**	90.4	86.8	**88.5**
		BAE	62.2	88.2	**91.7**	67.9	88.8	**90.3**
		Deepwordbug	—	83.4	**88.6**	—	83.3	**84.1**
	IMDB	TextFooler	77.4	94.8	**97.8**	83.8	95.0	**95.4**
		PWWS	70.5	**92.5**	92.0	80.0	92.4	**92.7**
		BAE	48.8	95.5	**96.9**	57.4	95.5	**97.7**
		Deepwordbug	—	92.0	**92.2**	—	**93.6**	91.5

Bold values indicate the optimal results among three defense methods.

is worth noting that in some settings (bold in Table 6), the detection effect is better than the default effect (the values in parenthesis in Table 6), which needs further exploration.

5. Qualitative Results and Discussion

5.1. Impact of Important Words. We choose the most important k words to represent the input text for feature extraction. In this subsection, we study the effect of varying the value of k on the detection effect. As shown in Figure 4, for IMDB, recall and $F1$-score remain high at $k \in [15, 30]$, and then decline; for AG's news, scores reach the highest point at $k = 5$. The results show that the best k values are different for texts and are tied to text length, and we suggest a range of $[0.1n, 0.2n]$ and n is the length of text.

5.2. Impact of Features. We consider the effects of selecting top k IWs, sensitivity signal marking, and probability distribution differences on the final detection performance. We use TextFooler + BERT as the invariant setting of the experiment to test the detection effectiveness on AG's news and IMDB with different feature selections. Table 7 shows the results of the ablation experiments, demonstrating that both the sensitivity signal and Softmax distribution inconsistency are effective as independent signals.

Table 4: Generalization evaluation of different attacks. Rec is recall, $F1$ is $F1$-score, R is the variation of the current adversarial recall rate relative to the default effect, and F is the variation of the current weighted average $F1$-score relative to the default effect. * denotes the baseline, which is the experimental setup for training the detector, followed by testing the detector against other attack methods with the same dataset and model.

Attack	CNN				LSTM				BERT			
	Rec (%)	&R (%)	$F1$ (%)	&F (%)	Rec (%)	&R (%)	$F1$ (%)	&F (%)	Rec (%)	&R (%)	$F1$ (%)	&F (%)
TextFooler*	99.2	*	96.3	*	97.8	*	95.4	*	97	*	97	*
PWWS	98.2	+0.1	96.0	+0.8	91.7	−0.7	91.8	−0.4	95.4	−2.0	96.8	+0.3
BAE	99.2	+1	96.3	+0.5	96.5	−0.1	95.0	−0.8	93.2	−2.8	94.6	−0.9
Deepwordbug	97.4	−0.8	94.8	−0.4	92.0	0	91.8	+0.4	93.2	−3.0	94.9	−1.0
TextFooler	99.0	−0.2	95.5	−0.8	97.4	−0.4	95.8	+0.4	97.5	+0.5	96.2	−0.8
PWWS*	98.1	*	95.2	*	92.4	*	92.2	*	97.4	*	96.5	*
BAE	98.8	+0.6	94.7	−1.1	97.2	+0.6	94.6	−1.2	95	−1.0	95.3	−0.2
Deepwordbug	97.8	−0.4	94.8	−0.4	92.2	+0.2	91.2	−0.2	94.6	−1.6	94.3	−1.6
TextFooler	98.8	−0.4	95.9	−0.4	96.9	−0.9	95.5	+0.1	97.4	+0.4	96.3	−0.7
PWWS	97.6	−0.6	96.4	+1.2	94.6	+2.4	93.9	+1.7	95.6	−1.8	95.7	−0.8
BAE*	98.2	*	95.8	*	96.6	*	95.8	*	96	*	95.5	*
Deepwordbug	97.0	−1.2	94.7	−1.1	91.0	−1.0	91.9	+0.5	95.6	−0.6	95.3	−0.6
TextFooler	99.4	+0.2	96.3	0	95.8	−2.0	95.1	−0.3	97.8	+0.8	96.6	−0.4
PWWS	97.6	−0.6	95.6	+0.4	93.6	+1.2	91.7	−0.5	95.0	−2.4	95.7	−0.8
BAE	98.6	+0.4	95.3	−0.5	95.1	−1.5	94.3	−1.5	93.8	−2.2	93.9	−1.6
Deepwordbug	98.2	*	95.2	*	92.0	*	91.4	*	96.2	*	95.9	*

Table 5: Transferability evaluation of different models. Bold values indicate the better scores among two target models that model* migrate to.

Model	TextFooler		PWWS		BAE		Deepwordbug	
	Recall (%)	$F1$-score (%)	Recall (%)	$F1$-score (%)	Recall (%)	$F1$-score (%)	Recall (%)	$F1$-score (%)
CNN*	99.2*	96.3*	98.1*	95.2*	98.2*	95.8*	98.6*	95.5*
LSTM	82.6	86.8	86.6	84.1	88.4	**90.9**	81.8	89.6
BERT	**89.2**	**93.8**	**91.6**	**92.6**	**90.4**	88.7	**89.7**	**92.5**
CNN	**98.5**	95.1	**99.9**	94.6	**97.5**	**94.8**	99.4	93.7
LSTM*	97.5*	95.4*	92.1*	92.2*	96.5*	95.5*	92.3*	91.6*
BERT	97.2	**95.7**	95.0	**95.2**	91.8	93.3	**94.8**	**94.7**
CNN	**99.1**	**96.1**	**100.0**	**93.7**	**97.1**	**96.3**	**98.7**	**96.0**
LSTM	95.4	95.2	92.2	91.4	96.2	95.5	95.4	94.7
BERT*	97.0*	97.0*	97.4*	96.5*	95.5*	95.5*	95.9*	95.9*

Nevertheless, the best results are achieved by combining them. Individual sensitivity signs alone do not work well in short texts; by contrast, Jensen-Shannon divergence calculated by Softmax distribution differences plays a greater influence. In addition, the selection of top k IWs improves detection performance by 5 – 8%.

5.3. Impact of Datasets.

Given the inconsistent capability of the detectors trained on IMDB and AG's news, we further explore exactly the key factor for this difference. The length of texts and the number of classes are two factors that are considered. In addition to the three datasets mentioned in Subsection 4.1, we add the SST-2 dataset as a reference experiment and split 5000 samples from the training set as the test set. Using four datasets and two baseline settings, we report the result in Table 8.

We observe a negligible difference in detection performance caused by the number of classes, but the data length matters detection performance a lot. We give a possible explanation for this phenomenon. In short-length texts with a small number of words, each word plays a more important role as texts have a small tolerance for information loss. As a result, perturbing each word in NEs affects higher fluctuations, so distinguishing between AEs and NEs becomes more challenging.

5.4. Challenges and Limitations.

We propose the universal feature of AEs: sensitivity inconsistency to important words being perturbed. However, various still exist in examples reacting to perturbation across different datasets and tasks. We acknowledge that the detection effect is somewhat weakened in short-length texts. We argue that fuller features

Table 6: Generalization evaluation in the toughest scenario. The values in parentheses are default effect. Bold values denotes that the detection performance under transferability is better than the default effect.

Dataset	Model	PWWS		BAE		Deepwordbug	
		Recall (%)	*F*1-score (%)	Recall (%)	*F*1-score (%)	Recall (%)	*F*1-score (%)
Yelp	LSTM	86.2 (91.6)	85.7 (90.5)	90.6 (94.5)	91.5 (93.2)	**92.8** (91.2)	**89.7** (87.4)
	RoBERTa	87.4 (94.7)	89.6 (92.6)	87.3 (92.0)	87.9 (92.7)	85.9 (92.8)	87.0 (89.1)
AG's news	LSTM	90.3 (94.4)	87.1 (88.5)	**93** (91.7)	**93.5** (90.3)	**91.4** (88.6)	**89.2** (84.1)
	RoBERTa	90.8 (91.3)	87.6 (85.4)	87.0 (89.9)	85.7 (91.2)	**88.9** (86.6)	**90.0** (87.5)

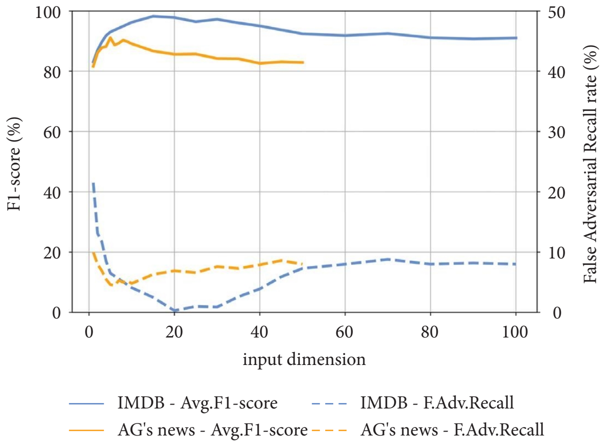


Figure 4: Detector performance under different value of k, which is equivalent to the input dimension.

Table 7: Detection performance of different features. None means features dimensionality is 300 for IMDB and 100 for AG's news; in top k settings, $k = 20$ for IMDB and $k = 5$ for AG's news.

Top k IWs	Sensitivity flags	Softmax distribution	IMDB		AG's news	
			Recall (%)	*F*1-score (%)	Recall (%)	*F*1-score (%)
None	✓		80.0	89.5	78.6	72.3
		✓	92.4	94.1	84.9	87.6
	✓	✓	92.0	91.5	90.1	90.5
k	✓		84.4	92.4	76.9	77.5
		✓	95.2	96.1	89.4	90.7
	✓	✓	**99.8**	**97.7**	**95.5**	**91.5**

Bold values indicate the best results in different feature settings.

Table 8: Performance of detector on different datasets.

Dataset	BERT + Deepwordbug		LSTM + TextFooler	
	Recall (%)	*F*1-score (%)	Recall (%)	*F*1-score (%)
IMDB	94.2	94.8	97.2	96.4
AG's news	85.0	85.6	96.2	91.2
Yelp	90.1	92	95.5	93.4
SST-2	81.2	84.3	87.6	89.1

are beneficial to further improve the performance of the detector.

IWs play a big role in prediction, so attackers utilize them to craft AEs, which is a common pattern of attack. While SIFD contains rich information from IWs to identify AEs, its detection performance will be severely limited if a stronger attack method breaks this pattern in the future. Aiming to escape this cat-and-mouse game, our future work includes exploring certifiable defense methods with formal guarantees.

The proposed method, SIFD, can work not only as a detection plug-in to assist the target model but also in combination with others. Theoretically, the generality of SIFD motivates it to be combined with robustness training to jointly enhance adversarial robustness from inside and outside the model. In further research, we will explore more application potentials of detection against adversarial attacks.

6. Conclusions

We propose an adversarial detection method named SIFD based on sensitivity inconsistency features (SIF) against perturbing important words, which contain rich information for identifying AEs in DNN-based IoHT systems. Different from previous methods that identified features of detection from the whole text, we focused on only the important parts, which are the key features of texts, and achieved better distinguishable signals. The proposed method effectively enhances the adversarial robustness of the DNN-based IoHT systems in analyzing textual data.

We evaluate SIFD with advanced adversarial detection methods against four attack methods (both character-level and word-level attacks are included), and the results show the superiority of our approach over currently available detection technologies. In addition, through a series of ablation experiments, we reveal the remarkable transferability of SIFD and analyze the importance of each local mechanism in SIF.

Data Availability

All the codes and datasets to reproduce our experimental results are open source at https://github.com/AuroraHuan/SIFD-adversrial-detection, and we hope they facilitate future research.

Additional Points

We confirm that this submission is not under consideration in any other journal, has not been published elsewhere, and is not currently under consideration by another journal.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Huan Zhang, Zhaoquan Gu, and Muhammad Shafiq were in charge of conceptualization; Huan Zhang, Bin Zhu, Hao Tan, and Muhammad Shafiq were in charge of methodology; Huan Zhang, Zhaoquan Gu, and Hao Tan were in charge of software; Huan Zhang was in charge of preparing the original draft; Zhaoquan Gu, Le Wang, and Bin Zhu were in charge of writing the review and editing; Zhaoquan Gu was in charge of funding acquisition; Muhammad Shafiq and Le Wang handled project administration; and Le Wang, Muhammad Shafiq, and Zhaoquan Gu supervised the study.

Acknowledgments

This work was supported in part by the Major Key Project of PCL (grant no. PCL2022A03), the Natural Science Foundation of China (grant no. 61902082), Guangzhou Science and Technology Planning Project (grant no. 202102010507), and the National Natural Science Foundation of China (grant no. 62250410365).

References

[1] Z. Gu, D. Li, N. Guizani, X. Du, and Z. Tian, "An aerial-computing-assisted architecture for large-scale sensor networks," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 43–49, 2021.

[2] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: a survey," *Sustainable Cities and Society*, vol. 60, pp. 102177–177, 2020.

[3] Z. Gu, Le Wang, X. Chen et al., "Epidemic risk assessment by a novel communication station based method," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 332–344, 2022.

[4] T. Cai, J. Li, A. S. Mian, R. H. Li, T. Sellis, and J. X. Yu, "Target-Aware holistic influence maximization in spatial social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 4, p. 1, 2020.

[5] Z. Gu, H. Li, S. Khan et al., "IEPSBP: a cost-efficient image encryption algorithm based on parallel chaotic system for green IoT," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 89–106, 2022.

[6] H. Tan, C. Liu, Y. Lyu, X. Zhang, D. Zhang, and Z. Gu, "Audio steganography with speech recognition system," in *Proceedings of the 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC)*, pp. 256–263, Shenzhen, China, October 2021.

[7] M. Shafiq, Z. Gu, N. Shah, and R. Yadav, "Analyzing IoT attack feature association with threat actors," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7143054, 11 pages, 2022.

[8] Z. Li, J. Xu, J. Zeng et al., "Searching for an effective defender: benchmarking defense against adversarial word substitution," in *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing (EMNLP) 2021*, pp. 3137–3147, Toronto, Canad, November 2021.

[9] C. Zhu, Y. Cheng, Z. Gan, S. Sun, T. Goldstein, and J. Liu, "Freelb: Enhanced adversarial training for natural language understanding," in *Proceedings of the 8th International Conference on Learningepresentations (ICLR)*, Addis Ababa, Ethiopia, April 2020.

[10] Di Jin, Z. Jin, T. Z. Joey, and S. Peter, "Is bert really robust? a strong baseline for natural language attack on text classification and entailment," in *Proceedings of the AAAI conference on artificial intelligence*, pp. 8018–8025, New York, NY, USA, February 2020.

[11] L. Li, R. Ma, Q. Guo, X. Xue, and X. Qiu, "Bert-attack: adversarial attack against bert using bert," in *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pp. 6193–6202, Toronto, Canada, October 2020.

[12] M. Ye, C. Gong, and Q. Liu, "SAFER: a structure-free approach for certified robustness to adversarial word substitutions," in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics (ACL)*, pp. 3465–3475, Toronto, Canada, July 2020.

[13] J. Zeng, X. Zheng, J. Xu, L. Li, L. Yuan, and X. Huang, "Certified robustness to text adversarial attacks by randomized [MASK," 2021, https://arxiv.org/abs/2105.03743.

[14] Y. Zhou, J.-Yu Jiang, K.-W. Chang, and W. Wang, "Learning to discriminate perturbations for blocking adversarial attacks in text classification," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, pp. 4903–4912, Toronto, Canada, November 2019.

[15] M. Mozes, P. Stenetorp, K. Bennett, and L. D. Griffin, "Frequency-guided word substitutions for detecting textual adversarial examples," in *Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics: Main Volume (EACL)*, pp. 171–186, Toronto, Canada, April 2021.

[16] E. Mosca, S. Agarwal, J. Rando-Ramirez, and G. Groh, "That is a suspicious reaction!': interpreting logits variation to detect NLP adversarial attacks," 2020, https://arxiv.org/abs/2204.04636.

[17] A. Fawzi, M.-D. Seyed-Mohsen, F. Pascal, and S. Soatto, "Empirical study of the topology and geometry of deep networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 3762–3770, Salt Lake City, UT, USA, June 2018.

[18] J. Tian, J. Zhou, Y. Li, and D. Jia, "Detecting adversarial examples from sensitivity inconsistency of spatial-transform domain," in *Proceedings of the 35th Conference on Artificial Intelligence (AAAI)*, pp. 9877–9885, Palo Alto, CA, USA, March 2021.

[19] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *Proceedings of the 3rd International Conference on Learning Representations (ICLR)*, San Diego, CA, USA, May 2015.

[20] A. Kurakin and J. Ian, "Goodfellow, and samy bengio, "adversarial examples in the physical world," in *Proceedings of the 5th International Conference on Learning Representations (ICLR)*, pp. 99–112, Toulon, France, April 2017.

[21] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and V. Adrian, "Towards deep learning models resistant to adversarial attacks," in *Proceedings of the 6th International Conference n Learning Representations (ICLR)*, Vancouver, BC, Canada, May 2018.

[22] Z. Gu, W. Hu, C. Zhang, H. Lu, L. Yin, and Le Wang, "Gradient shielding: towards understanding vulnerability of deep neural networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 921–932, 2021.

[23] S. Samanta and S. Mehta, "Towards crafting text adversarial samples," 2017, https://arxiv.org/abs/1707.02812.

[24] B. Liang, H. Li, M. Su, B. Pan, X. Li, and W. Shi, "Deep text classification can be fooled," 2017, https://arxiv.org/abs/1704.08006.

[25] J. Ebrahimi, A. Rao, L. Daniel, and D. Dou, "Hotflip: white-box adversarial examples for text classification," in *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (ACL)*, pp. 31–36, Melbourne, Australia, November 2018.

[26] S. Ren, Y. Deng, K. He, and W. Che, "Generating natural language adversarial examples through probability weighted word saliency," in *Proceedings of the 57th annual meeting of the association for computational linguistics(ACL)*, pp. 1085–1097, Florence, Italy, August 2019.

[27] S. Garg, G. Ramakrishnan, and Bae, "Bert-based adversarial examples for text classification," in *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pp. 6174–6181, Punta Cana, January 2020.

[28] Ji Gao, J. Lanchantin, M. Lou Soffa, and Y. Qi, "Black-box generation of adversarial text sequences to evade deep learning classifiers," in *Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW)*, pp. 50–56, San Francisco, CA, USA, May 2018.

[29] Y. Zang, F. Qi, C. Yang et al., "Word-level textual adversarial attacking as combinatorial optimization," in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics (ACL)*, pp. 6066–6080, Toronto, Canada, July 2020.

[30] B. Zhu, Z. Gu, Y. Qian, F. Lau, Z. Tian, and Z. Tian, "Leveraging transferability and improved beam search in textual adversarial attacks," *Neurocomputing*, vol. 500, pp. 135–142, 2022.

[31] R. Maheshwary, S. Maheshwary, and V. Pudi, "Generating natural language attacks in a hard label black box setting," in *Proceedings of the 35th Conference on Artificial Intelligence (AAAI)*, pp. 13525–13533, Palo Alto, CA, USA, February 2021.

[32] M. Ye, C. Miao, T. Wang, and F. Ma, "TextHoaxer: budgeted hard-label adversarial attacks on text," in *Proceedings of the 36h Conference on Artificial Intelligence (AAAI)*, pp. 4844–1852, Washington, DC, USA, February 2022.

[33] A. Azizi, T. Ibrahim Asadullah, A. Waheed et al., "A generative approach to defend gainst trojan attacks on DNN-based text classification," in *Proceedings of the 30th USENIX Security Symposium (USENIX Security)*, pp. 2255–2272, Berkeley, CA, USA, August 2021.

[34] T. Miyato, A. M. Dai, and I. Goodfellow, "Adversarial training methods for semi-supervised text classification," in *Proceedings of the 5th International Conference on Learning Representations (ICLR)*, Toulon, France, April 2017.

[35] L. Li and X. Qiu, "Tavat: token-aware virtual adversarial training for language understanding," 2020, https://arxiv.org/abs/2004.14543.

[36] E. Jones, R. Jia, A. Raghunathan, and P. Liang, "Robust encodings: a framework for combating adversarial typos," in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pp. 2752–2765, Toronto, Canada, July 2020.

[37] C. Si, Z. Zhang, F. Qi et al., "Better robustness by more coverage: adversarial and mixup data augmentation for robust finetuning," in *Proceedings of the Findings of the Association for Computational Linguistics: ACL-IJCNLP*, pp. 1569–1576, Toonto, Canada, August 2021.

[38] B. Zhu, Z. Gu, Le Wang, J. Chen, and X. Qi, "Improving robustness of language models from a geometry-aware perspective," 2022, https://arxiv.org/abs/2204.13309.

[39] X. Wang, H. Jin, Y. Yang, and K. He, "Natural language adversarial defense through synonym encoding," in *Proceedings of the 37th Conference on Uncertainty in Artificial Intelligence (UAI)*, pp. 823–833, Baltimore, Maryland, June 2021.

[40] B. Liang, H. Li, M. Su, X. Li, W. Shi, and X. Wang, "Detecting adversarial image examples in deep neural networks with adaptive noise reduction," *IEEE Transactions o Dependable and Secure Computing*, vol. 18, no. 1, pp. 72–85, 2021.

[41] Y. Wang, L. Xie, X. Liu, J.-Li Yin, and T. Zheng, "Model-agnostic adversarial example detection through logit distribution learning," in *Proceedings of the 2021 IEEE International Conference on Image Processing (ICIP)*, pp. 3617–3621, Anchorage, AK, USA, September 2021.

[42] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT)*, pp. 4171–4186, Minneapolis, MN, USA, June 2019.

[43] A. Maas, R. E. Daly, P. T. Pham, D. Huang, A. Y. Ng, and C. Potts, "Learning word vectors for sentiment analysis," in *Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies*, pp. 142–150, Portland, Oregon, June 2022.

[44] X. Zhang, J. Zhao, and Y. LeCun, "Character-level convolutional networks for text classification," in *Proceedings of the Advances in Neural Information Processing Systems*, pp. 649–657, Quebec, Canada, USA, December 2015.

[45] Y. Liu, M. Ott, N. Goyal et al., "A robustly optimized bert pretraining approach," 2019, http://arxiv.org/abs/1907.11692.

[46] Ye Zhang and B. Wallace, "A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification," in *Proceedings of the 8th International Joint Conference on Natural Language Processing (IJCNLP)*, pp. 253–263, Taipei, Taiwan, November 2017.

[47] S. Hochreiter and J. Schmidhubr, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[48] J. Pennington, R. Socher, and C. D. Manning, "Glove: global vectors for word representation," in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, pp. 1532–1543, Doha, Qatar, October 2014.

[49] T. Chen and C. Guestrin, "Xgboost: a scalable tree boosting system," in *Proceedings of the 22nd international conference on knowledge discovery and data mining*, pp. 785–794, San Francisco, CA, USA, August 2016.

[50] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[51] G. Ke, M. Qi, T. Finley et al., "A highly efficient gradient boosting decision tree," in *Proceedings of the Annual Conference on Neural Information Processing Systems 2017*, pp. 3146–3154, Long Beach, CA, USA, December 2017.

[52] M. A. Hearst, S. T. Dumais, E. Osuna, J. Platt, and B. Scholkopf, "Support vector machines," *IEEE Intelligent Systems and Their Applications*, vol. 13, no. 4, pp. 18–28, 1998.

[53] R. E. Schapire, "A brief introduction to boosting," in *Proceedings of the 16th International Joint Conference on Artificial Intelligence (IJCAI)*, pp. 1401–1406, Stockholm, Sweden, August 1999.

Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 1044282, 15 pages
https://doi.org/10.1155/2023/1044282

Research Article

A Lightweight Three-Party Mutual Authentication Protocol for Internet of Health Things Systems

Zhihui Wang,[1] **Jianli Zhao**,[2] **Peng Sun**,[1] **Jingjing Yang**,[1] **Rui Wang**,[1] **and Xiao Zhang**[1]

[1]*Hebei North University, Zhangjiakou 07500, Hebei, China*
[2]*State Grid Hebei Electric Power Research Institute, Shijiazhuang 050000, Hebei, China*

Correspondence should be addressed to Xiao Zhang; xzh1965@hebeinu.edu.cn

Received 10 February 2022; Revised 11 April 2022; Accepted 15 April 2022; Published 22 February 2023

Academic Editor: Muhammad Asghar Khan

In Internet of Health Things (IoHT) systems, there is a two-hop network structure between the authentication server TA, Internet of Things Connector (IotC), and wearable sensor (WS). Attackers can use the sensor layer network (the first hop) between the IotC and WS to steal patient's health-related information and undermine the security of the system and the privacy of sensitive information. To address this threat, this study proposes a lightweight identity authentication and key agreement protocol for third-party authentication servers TA, IotC, and WS. The results of the formal security proof, BAN logic analysis, and AVISPA tool simulation show that the scheme proposed in this study has an ideal security performance and can meet the security requirements of IoHT. In terms of performance, the proposed scheme could dynamically construct a sensor layer network (the first hop) and offline networking according to the diagnostic needs of doctors. Compared with other related protocols, the proposed scheme can significantly reduce the computing resource requirements of IotC and server TA and the resource requirements of database I/O operation of server TA in the application scenario of concurrent access of multiple WS nodes.

1. Introduction

The wearable technology market has reached US $116.2 billion in 2020 and is expected to increase to US $265.4 billion by 2026, with an annual compound growth rate of 18.0% [1]. The rapid growth of the market scale of wearable technology is also constantly promoting the integration of wearable or implantable device technology with IoT, cloud computing, and other information technologies into Internet of Health Things (IoHT) systems in the hospital environment [2]. These new technologies can help medical professionals obtain various types of health data information of target patients faster and better [3] and help medical institutions continuously improve the quality of medical services [4].

Figure 1 describes the general network structure of IoHT systems applied in the medical structure environment [5–8]. Its remarkable feature is the integration of the IoT, cloud computing, wearable, or implantable device technology. As shown in Figure 1, an IoHT system is composed of two interconnected network units: a data service unit and IoT unit. They are connected through a common set of cloud data storage servers.

The IoT unit is a two-hop network structure, similar to the IEEE 802.15.6 Wireless Body Area Network (WBAN) standard description [9] and the industrial Internet of Things [10]. Multiple wearable sensors (WSs) and Internet of Things Connectors (IotCs) constitute the first hop of an IoHT system, that is, the sensor layer network. The IotC and local real-time data monitoring terminal (LMT) or cloud data server form the second-hop transport layer network. In terms of function, it emphasizes the ability of real-time, fast, and accurate acquisition and two-way data transmission of Patient Health Information (PHI) [5, 8, 11], such as patient activity, blood pressure, heart rate, electrocardiogram (ECG), temperature, blood glucose, and blood oxygen level [12].

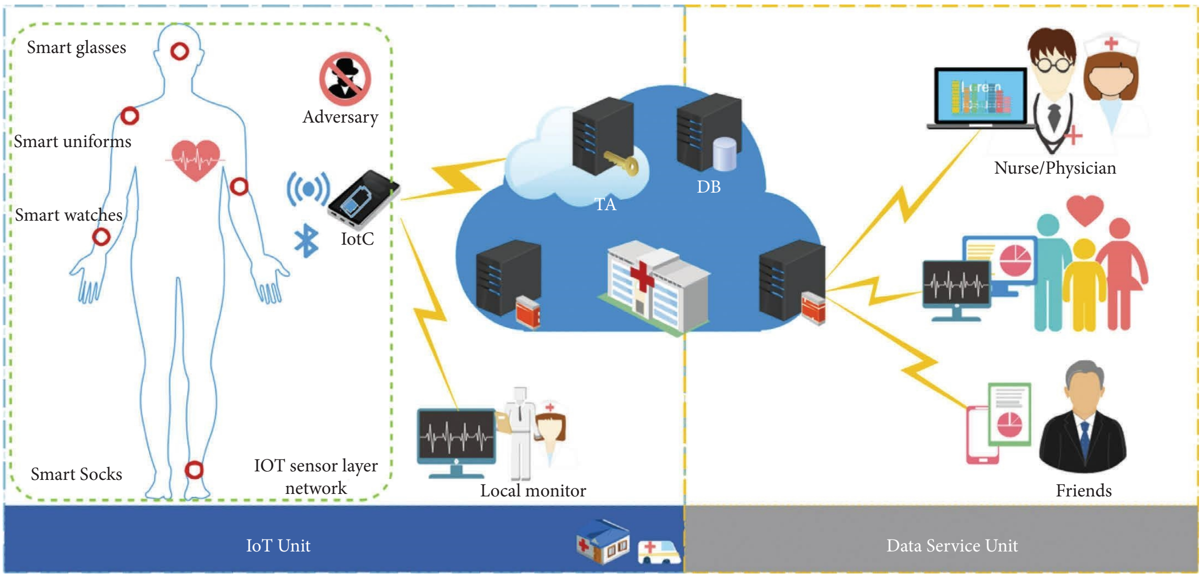


Figure 1: Network structure of the IoHT system.

1.1. Networking Requirements of Sensor Layer Networks. The main application environment of IoHT systems is the medical institutions that provide public medical and health services. Patients have a strong mobility and various other conditions. Therefore, the IoHT systems must collect the corresponding PHI data according to a patient's condition such as monitoring of blood glucose levels and blood pressure. Some data require a high real-time performance, such as heart rate data in intensive care or cardiac care environments. These have put forward the following special functional requirements or limitations for the network structure of the sensing layer of the IoHT systems:

(i) WS and IotC are small in size, easy to carry, and have limited computing resources; therefore, they are not suitable for jobs with a high amount of computing [13].

(ii) The correspondence between the patients and IotC was variable. The IotC ownership in IoHT systems is a medical institution that has a corresponding relationship with patients within a certain time range.

(iii) The types and number of WS nodes are large, and the server in the IoHT systems should have strong equipment access capability.

(iv) The WS nodes are rarely used in isolation. In most cases, these groups were included. IotC should be able to concurrently network multiple WSs.

(v) The combination of IotC and WS must be built according to the diagnostic needs of doctors [7].

(vi) To reduce the impact of remote network quality on IoHT system availability, the IotC and WS should have offline networking capabilities.

1.2. Requirements of IoHT Systems Lightweight Authentication Strategy. The correctness, timeliness, and credibility of PHIs can support doctors' decision making and help save or prolong patients' lives [14]. However, many theft events in PHI data [4] make the security of PHIs a hot issue for healthcare organizations. The Health Insurance, Portability, and Accounting Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) require all healthcare organizations to ensure the safety of health information.

Network attacks against IoT terminal devices, such as webcams [15], small routers [16], bluetooth door locks [17], intelligent thermostats [18], and theft of face recognition data [19], have made people gradually realize that IoT devices in IoHT systems may become a tool for attackers to launch network attacks and destroy the stability of IoHT systems or steal user-sensitive information.

The mutual Authentication and Key Agreement (AKA) mechanism between IoT access devices is an important link for building a secure health system (SHS) [20]. The VPN, SSL, TLS, and other security mechanisms are based on the Internet peer-to-peer communication mechanism, which can ensure data security on both sides, for example, the establishment of a secure data channel between the IotC and the data server [21]. However, because of the two-hop network structure of the IoT unit of IoHT systems and the networking requirements of the sensor layer network, it is very difficult to use VPN, SSL, TLS, and other protocols to build a mutual AKA in the first-hop network (sensor layer network). Therefore, the IoHT systems require a lightweight, anonymous, and secure mutual AKA protocol, that is, more suitable for network structures [22].

2. Related Work

The special structure and functional requirements of IoHT systems restrict their application in traditional security protocols. To deal with the threat of malicious attacks, improve the security level of IoHT systems, and meet the functional requirements of portable and ultralow power consumption of wearable sensors, various lightweight mutual AKAs have been proposed.

In 2015, He and Zeadally proposed a lightweight three-party authentication protocol to improve the identity authentication ability of controllers in ambient-assisted living systems [23]. Subsequently, in 2016, with the help of a third-party authentication server, He et al. realized lightweight identity authentication of users using a data aggregation device in the smart grid [24]. The two protocols are based on the elliptic curve (EC) theory and realize the support of third-party authentication servers; therefore, they have low overall resource consumption and high security, but the individual resource consumption of the controller is still high, and the support for sensing devices is insufficient.

In 2017, Li et al. [9] proposed an anonymous lightweight identity authentication and key agreement protocol for two-hop wireless body area networks (WBANs). The protocol is based on a hash function and XOR computing, which significantly reduces the demand for computing resources for wireless sensor devices. A hub node must undertake multiple functions, such as identity authentication, real-time data monitoring, data storage, and remote cloud data forwarding, which are not conducive to the implementation of a security protection strategy, is easier to capture, and has a single point of failure.

In 2018, Srinivas et al. [6] proposed a lightweight tripartite authentication scheme for WSs, users, and cloud servers based on cloud computing and big-data technology. The security of the scheme is verified using a formal real or random (ROR) model and the automatic verification tool AVISPA [25]. This scheme has significant advantages in terms of the communication and computing costs.

However, Srinivas' protocol must store the authentication information $\langle \mathrm{HID}_i, TC_{ji2} \rangle$ of all possible users in the memory of all the WSs in advance. This causes the wearable sensor of the protocol to have a large demand for storage resources and insufficient ability to resist WS theft attacks [16]. Simultaneously, we found that the construction of the sensor layer network of the protocol requires more manual processing, which is more suitable for networks with stable structures. Under the demand for on-demand construction of an IoHT system sensor layer network, labor and system maintenance costs will increase.

To enhance the ability of wearable devices to protect sensitive data and resist WSs theft attacks, Das et al. [5] proposed a lightweight tripartite authentication and session key scheme between WSs and mobile terminals (MT) (i.e., smartphones) carried by the same user. The security of the protocol was verified using a real or random model and AVISPA tool. Compared with the previous scheme, this method has certain advantages in terms of resource consumption. However, Jiang et al. [26] pointed out that the Das scheme does not resist offline password-guessing attacks, and attackers can use desynchronization attacks to destroy the synchronizer of identity update between WS and MT [26] and provided an improved scheme. Jiang's scheme offers advantages in terms of security and resource consumption. However, we also found that there were still some problems with Jiang's scheme.

(i) This method is suitable for application in personal health monitoring. In Jiang's scheme, the user is an MT and the WS is the owner, who lacks the basic function of adjusting the combination relationship of the user, MT, and WSs according to the patient's condition and the doctor's diagnostic needs.

(ii) There is a security risk in the denial-of-service (DOS). In Jiang's protocol, MT lacks the necessary verification for message M1, so attackers can use this to send many wrong M1, thus exhausting the computing, communication, and server database I/O resources of MT and the cloud server (CS) to achieve the purpose of DOS.

(iii) The computing resource requirements for concurrent MT access to multiple WS nodes must be improved. When the MT needs to access multiple WS nodes, the MT and CS have more repeated calculations and higher demand for computing resources.

(iv) The capability of offline networking between MTs and WSs must be improved. In the process of accessing the WS, the server CS must be online and provide corresponding services.

(v) The CS has a high demand for I/O database resources. Each time the MT accesses the WS, at least three queries and one database update operation are required. In an IoHT system environment, this may lead to a shortage of CS database resources, affect the number of WS nodes accessed, and weaken the server's ability to resist DoS attacks.

To enhance the ability of identity authentication between the Internet of Things connector (IotC) and local real-time data terminal, Srinivas et al. proposed a novel temporal credential-based anonymous lightweight user authentication mechanism for the Internet of Drones (IoD) environment [27]. The security of the scheme is proved using a real or random (ROR) model and automated validation of Internet security protocols and applications (AVISPA). However, this scheme does not support the dynamic construction of a sensor layer network. In 2020, Wang et al. [7] proposed a lightweight WSs and WNC mutual authentication protocol based on the elliptic curve cryptography (ECC) algorithm. With the help of a cloud-assisted authentication service, the protocol can realize mutual authentication and key negotiation of a wearable network connector (WNC) access to WSs designated by doctors. However, this scheme has shortcomings in terms of protection against ID. The attacker uses this to track the specified WSs and obtain sensitive data by analyzing the communication frequency and data volume. However, compared to the schemes of Srinivas, DAS, and Jiang, the resource consumption of their sensing terminals remains high.

3. Preliminaries

3.1. Elliptic Curve (EC). Let E be an elliptic curve over a finite field F_p defined by the following equation: $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$, where $x, y, a, b \in F_p$ and $(4a^3 + 27b^2)\mathrm{mod}\, p \neq 0$. $E(F_p)$ represents a cyclic group constructed from points on elliptic curve E and infinity ∞.

3.2. Scalar Multiplication. When $P \in E(F_p)$, there is a multiplication formula: $t \cdot P = P + P + \ldots + P\,(t \text{ times})$ holds.

3.3. Elliptic Curve Discrete Logarithm Problem (ECDLP). When $P \in E(F_p)$ and integer t are known, it is easy to calculate $= t \cdot P$, where $Q \in E(F_p)$. When Q and P are known, it is very difficult to calculate the value of the integer t.

3.4. Elliptic Curve Cryptography (ECC). A public-key algorithm based on ECDLP security is called elliptic curve cryptography (ECC). Compared with RSA, ECC requires fewer computing and storage resources [28, 29].

3.5. Elliptic Curve Diffie–Hellman Discrete Logarithm Problem (ECDHDLP). Assuming $c, d \in F_p$ and $G, c \cdot G, d \cdot G \in E(F_p)$, when the values of c and $d \cdot G$ or d and $c \cdot G$ are known, it is easy to calculate $c \cdot d \cdot G \in E(F_p)$, but when $c \cdot G$ and $\mathrm{d} \cdot G$ are known, it is very difficult to calculate $c \cdot d \cdot G$.

3.6. Fuzzy Extractor (FE). This is a highly secure biometric recognition method. It contains $(\delta_i, \tau_i) = \mathrm{Gen}(\mathrm{Bio}_i)$ and $\delta'_i = \mathrm{Rep}(\mathrm{Bio}'_i, \tau_i)$ functions [5], where $\mathrm{Bio}_i, \delta_i, \tau_i \in 0, 1^l$. When the deviation between Bio'_i and Bio_i is less than t, $\delta_i = \delta'_i$ can be obtained.

3.7. Collision-Resistant Hash Function. The hash function can convert any long input string $\{0, 1^*$ into a fixed-length value $\{0, 1^L$. If the hash values of two different input strings are the same, the two strings form a set of hash collisions. $Adv_{HASH}(\mathscr{A})$ denotes the advantage of adversary $\mathscr{A}$ in identifying hash collisions: when $\mathrm{Adv}_{\mathrm{HASH}}(\mathscr{A}) \leq \varepsilon$, ε is a real number sufficiently small to be ignored. This hash function is called a collision-resistant hash function.

3.8. Parameters and Symbols. Table 1 lists the names and descriptions of parameters, methods, and symbols required by the proposed protocol. To prevent replay attacks, all participants in the IoHT system network have their own independent timing unit, T, and can maintain synchronization with the system clock of the IoHT systems.

4. The Proposed Scheme

Mutual authentication protocols between devices are typically based on mutually trusting secret information [30]. The combined relationship between patients and IotC and between IotC and WS in IoHT systems often needs to be changed, and the resources of IotC and WS are limited and very different. In this case, the three-party mutual authentication scheme, including the third-party server TA, has clear advantages in terms of communication and storage resources [30]. Therefore, based on the ECDLP and hash function, we propose a lightweight AKA scheme that uses anonymous third-party devices.

4.1. Devices Registration. Figure 2 describes the registration process of IotC. At this stage, TA records the IotC identity and generates a new authentication code TC_i. The numerical numbers of (1), (2), . . ., (7) in Figure 2 are in the order in which IotC and TA execute the protocol at this stage. To enhance the flexibility of the administrator's workplace, we have strengthened the security protection of the communication process. For example, the tracking of equipment is prevented by formulas $ID_i^* = ID_i \oplus h(B \| T_{i1})$ and $D_i = ?I D_i^* \oplus h(B_x \| T_{s1})$; TA calculates $V = ?h(ID_i \| PW_i \| B \| T_{i1})$, and the identity authentication of IotC and administrator users is realized. The registration process of WS is similar to that described in Figure 2.

4.2. IotC Binding to a Patient. The corresponding relationship between the patient and the IotC in the IoHT systems is variable. IotC has only a corresponding relationship with the patient within a certain time range. To meet this demand, this study proposed a strategy for binding IotC_i to a patient. During the validity period, IotC_i and the server TA (PID, PTC) were used to mark the correspondence between IotC_i and the patient. Figure 3 shows the detailed process of binding IotC_i receptor binding to a patient. Numerical numbers such as "(1), (2), . . ., (5)" in Figure 3 are the execution sequences of IotC_i and TA in this stage.

(1) IotC_i local authentication administrator.

(2) IotC_i requests and determines the patient information. In this process, the formula $ID_i^* = ID_i \oplus h(B \| T_{i2})$ is used to encrypt the ID of IotC_i to prevent device tracking.

(3) TA authenticates IotC_i. TA uses the formula $B' = S_{TA} \cdot A$ to calculate the ID decryption key of IotC_i. IotC identity is verified using $V_1 = ?h(ID'_i \| TC_i \| A \| T_{i2})$.

(4) TA binds a patient to IotC_i. The TA selects a user userID and calculates $\mathrm{PID} = h(ID'_i \| \mathrm{user}ID \| c \| T_{S2})$ and $\mathrm{PTC} = h(PID \| TC_i \| T_{S2} \| B')$.

(5) IotC_i binds a patient. After receiving message M_4, IotC_i uses the information to calculate PID and PTC. Subsequently, the key is calculated using the formulas $\mathrm{Gen}(\mathrm{Bio}_n) = (\delta_n, \tau_n)$ and $UK = h(ID_i \| \delta_n)$, and the PID and PTC are encrypted and saved using the formula $w_n = E_{UK}(\mathrm{PID}, \mathrm{PTC}')$.

4.3. TA Authorizes IotC. The ability of the sensor layer network to support the patient's condition and the doctor's diagnosis requires variable correspondence between a patient and multiple WS nodes. This relationship can be replaced by that between $IotC_i$ and multiple WS nodes after the patient is bound to IotC_i.

Therefore, this study proposes a strategy for TA to authorize IotC to access WS nodes and use (NID, AC [1, . . ., n]) to mark the corresponding relationship between an IotC and multiple WS nodes. Figure 4 describes the process of IotC_i obtaining the access authorization of a WS node. When multiple WS nodes require access, the variable Ac_j is an array.

Table 1: Parameters, methods, and symbols.

Notation	Description	Notation	Description
TA	Cloud authentication server	IotC	A wearable Internet of Things connector
s_{TA}, P_{TA}	Server key pair $P_{TA} = s_{TA} \cdot G$	Δt, ΔT	Effective time
WS	A wearable device	T_i	Current time of device i
G	Selected elliptic curve base point	$= ?$	Determine whether they are equal
status	Status of equipment	$\oplus$	XOR operation
$\|\|$	Concatenation operation	SK	Session key
PID	Temporary ID of the patient after binding with IotC	PTC	Temporary identification code of the patient after binding with IotC
NID	Temporary network ID authorized by TA	Ac	Temporary authentication code authorized by the server
a, c, x, y	Random parameters	$h()$	Collision-resistant hash function
TC_i	Authentication code of device I	PW_i	Management key for device i
Bio	User's biometric information	Rep $(\cdot)$	Deterministic reproduction function
Gen (.)	Probabilistic generation function	τ	Reproduction parameter from $Gen(.)$
δ	Biometric key from Gen (.)	E ()/D ()	Encryption/decryption method

$IotC_i$	Server TA
1) $read: \{P_{TA}, PW_i\}$	3) received M_1
2) $select: a, A = a \cdot G, B = a \cdot P_{TA}$	$\|T_{i1} - T_{s1}\| <\triangle t$
$ID^*{}_i = ID_i \oplus h(B\|\|T_{i1})$	$B' = s_{TA} \cdot A$
$V = h(ID_i\|\|PW_i\|\|B\|\|T_{i1})$	$ID_i = ID^*{}_i \oplus h(B'\|\|T_{i1})$
send $M_1: \{ID^*{}_i, A, T_{i1}, V\}$.	$search: status, PW_i\ by\ ID'{}_i$
	$V =? h(ID_i\|\|PW_i\|\|B\|\|T_{i1})$
6) receive M_2	4) $select: c, C = c \cdot \mathrm{G}$
$ID_i =? ID^*{}_i \oplus h(B_x\|\|T_{s1})$	$Q = c \cdot A$
$Q' = a \cdot \mathrm{C}$	$ID^*{}_i = ID_i \oplus h(B'_x\|\|T_{s1})$
$\mathrm{TC_i} = \mathrm{h}(ID_i\|\|Q'\|\|T_{s1})$	$\mathrm{T}C_i = \mathrm{h}(ID_i\|\|Q\|\|T_{s1})$
$V_0 =? \mathrm{h}(ID_i\|\|TC'_i\|\|T_{s1}\|\|Q')$	5) $V_0 = \mathrm{h}(ID_i\|\|TC_i\|\|T_{s1}\|\|Q)$
7) $f_i = TC'_i \oplus h(ID_i\|\|PW_i)$	$store: \{ID_i, TC_i\}$
$e_i = h(PW_i \oplus ID_i)$	$send\ M_2: \{ID^*{}_i, C, V_0, T_{s1}\}$
$store: P_{TA}, f_i, e_i$	

Figure 2: IotC registration phase.

$IotC_i$	Server TA
1) $read\ \ PW_i$	
$e_i =? h(PW_i \oplus ID_i)$	3) $receive\ M_3$
2) $TC'_i = f_i \oplus h(ID_i\|\|PW_i)$	$get: T_{S2}, \|T_{i2} - T_{S2}\| <\triangle t$
$select: a, A = a \cdot G, B = a \cdot P_{TA}$	$B' = S_{TA} \cdot A$
$ID^*{}_i = ID_i \oplus h(B\|\|T_{i2})$	$ID'{}_i = ID^*{}_i \oplus h(B'\|\|T_{i2})$
$V_1 = h(ID'{}_i\|\|TC_i\|\|A\|\|T_{i2})$	$search: ID'{}_i\ get\ TC_i$
$send\ M_3: \{ID^*{}_i, A, V_1, T_{i2}\}$	$V_1 =? h(ID'{}_i\|\|TC_i\|\|A\|\|T_{i2})$
	4) $Find: userID$
5) $received\ \ M_4$	$Select: c$
$PID = PID^* \oplus h(B\|\|T_{i2})$	$PID = h(ID'{}_i\|\|userID\|\|c\|\|T_{S2})$
$V_2 =? h(PID\|\|TC'{}_i\|\|T_{S2})$	$PID^* = PID \oplus h(B'\|\|T_{i2})$
$User\ Input\ Bio_n$	$PTC = h(PID\|\|TC_i\|\|T_{S2}\|\|B')$
$Gen(Bio_n) = (\delta_n, \tau_n)$	$Store: \{PID, PTC\}$
$u_n = \mathrm{h}(\mathrm{ID}_i\|\|\delta_n\|\|\tau_n)$	$V_2 = h(PID\|\|TC_i\|\|T_{S2})$
$PTC' = h(PID\|\|TC'_i\|\|T_{S2}\|\|B)$	$send\ M_4: \{PID^*, V_2, T_{S2}\}$
$UK = h(ID_i\|\|\delta_n)$	
$w_n = E_{UK}(PID, PTC')$	
$Store: \{u_n, \tau_n, w_n\}$	

Figure 3: IotC binding patient process.

4.4. IotC Offline Access to WS Node. IoHT systems must meet the needs of offline construction of the sensor layer network in real working scenarios. Therefore, this study proposes a strategy in which TA authorizes once, and IotC can access the specified WS node offline many times within the authorization time range. Figure 5 describes the implementation process of the AKA policy of IotC$_i$ offline access to WS_j.

(1) IotC$_i$ authenticates the users locally. IotC$_i$ verifies the user's identity by using the fuzzy extractor function and decrypts and calculates the NID, Ac_j, and T_{s3}, which are required to access WS_j.

$IotC_i/patient_i$	Server TA
1) Input and $\delta'{}_n = Rep(Bio_n, \tau_n)$	
$u_n =? h(ID_i\|\|\delta'{}_n\|\|\tau_n)$	*2)* … $\Longrightarrow: M_5$
$UK = h(ID_i\|\|\delta'{}_n)$	$get: T_{s3}, /T_{i3} - T_{s3}\| <?\triangle t$
$\{PID, PTC'\} = D_{UK}(w_n)$	$B' = S_{TA} \cdot A$
$select: a, A = a \cdot G, B = a \cdot P_{TA}$	$PID = PID^* \oplus h(B'\|\|T_{i3})$
$PID^* = PID \oplus h(B\|\|T_{i3})$	$\|T_{s2} - T_{s3}\| <?\triangle T$
$V_3 = h(PID\ \|\|T_{i3}\|\|PTC'\|\|A)$	$search: PTC, WS_j\ by\ PID$
$M_5: \{PID^*, A, V_3, T_{i3}\} \quad \Longrightarrow TA$	$V_3 =? h(PID\|\|T_{i3}\|\|PTC\|\|A)$
	3) $select: c, C = c \cdot G, Q = c \cdot A$
4) $Q' = a \cdot C \qquad M_6: \Longleftarrow TA$	$NID = h(PID\|\|Q\|\|PTC\|\|T_{s3})$
$Ac_j = E_j \oplus h(Q'\|\|PTC'\|\|T_{s3})$	$Ac_j = h\big(NID\|\|ID_j\|\|TC_j\|\|T_{s3}\big)$
$V_4 =? h\big(Q'\|\|Ac_j\|\|T_{s3}\|\|PTC\big)$	$E_j = Ac_j \oplus h(Q\|\|PTC\|\|T_{s3})$
$NID' = h(PID\|\|Q'\|\|PTC'\|\|T_{s3})$	$V_4 = h\big(Q\|\|Ac_j\|\|T_{s3}\|\|PTC\big)$
$w_n = E_{UK}\big(PID, PTC', NID, Ac_j, T_{s3}\big)$	$\Longleftarrow M_6: \{C, V_4, E_j, T_{s3}\}$
$Store: w_n$	

Figure 4: TA authorizes IotC$_i$ access to WS node.

(2) Login WS_j. IotC$_i$ calculates the variable values of TID, Y, T_{s3}, and V_5 in turn. Message M_7 is combined and broadcast to the sensor layer network.

(3) WS_j verifies IotC$_i$. After receiving message M_7, WS_j uses the formula $|T_j - T_{s3}| < \triangle T$, $|T_j - T_{i4}| < \triangle t$ to verify the authorization validity $\triangle T$ and data transmission validity $\triangle t$, and $\triangle T$ is much greater than $\triangle t$. Then, WS_j uses the formula $h(TID_j \| UID \| Ac_j \| T_{s3} \| T_{i4} \| h(y))$ to verify the access authorization of IotC$_i$.

(4) Calculate the session key SK. After the identity authentication of IotC$_i$ is successful, WS_j uses the formula $SK_{ij} = h(h(x) \| h'(y) \| Ac'_j \| T_{i4})$ to calculate the session key SK_{ij} between WS_j and $IotC_i$. WS_j continues to calculate the values of variables X and V_6 and returns the message M_8 to IotC$_i$.

(5) IotC$_i$ authenticates WS_j. After receiving the message M_8, IotC$_i$ uses the formula $|T_j - T_{i4}| < \triangle t$ to verify the time validity of the message. If valid, IotC$_i$ using TID$_j$ in the current message, select Ac'_j corresponding to sending message M_7 and calculate $SK'_{ij} = h(h'(x) \| h(y) \| Ac'_j \| T_{i4})$ to obtain SK'_{ij}. Then, calculate $\{ID_j, T_j, h'(y)\} = D_{SK}(V_6)$. If equation $h'(y) = ?h(y)$ holds, IotC$_i$ successfully authenticates WS_j identity.

4.5. IotC Online Access WS. In the proposed scheme, when IotC obtains access authorization for the WS, the process of accessing the specified WS for the first time can be regarded as an online access. That is, after IotC completes all the operations described in Figure 4 and obtains NID, Ac_j, and T_{s3}, it can directly transfer to the number "(2)" in Figure 5, mark the part, and begin to enter the WS node.

$IotC_i/patient$	Wearable Device WS_j
$1)\ Input\ and\ \delta'_n = Rep(Bio_n, \tau_n)$	
$u_n =?\ h(ID_i \Vert \delta'_n \Vert \tau_n)$	$3) \dots \Longrightarrow M_7$
$UK = h(ID_i \Vert \delta_n)$	$\lvert T_j - T_{s3} \rvert < \triangle T, \lvert T_j - T_{i4} \rvert < \triangle t$
$(NID, Ac_j, T_{s3}) = D_{UK}(w_n)$	$Ac'_j = h(NID \Vert ID_j \Vert TC_j \Vert T_{s3})$
$2) Select: y, Y = h(y) \oplus h(Ac_j \Vert T_{i4})$	$h'(y) = Y \oplus h(Ac'_j \Vert T_{i4})$
$select: TID_j \in \{0,1\}^{32}$	$V_5 =?\ h(TID_j \Vert NID \Vert Ac'_j \Vert T_{s3} \Vert T_{i4} \Vert h'(y))$
$V_5 = h(TID_j \Vert NID \Vert Ac_j \Vert T_{s3} \Vert T_{i4} \Vert h(y))$	$4) select: x$
$M_7: \{TID_j, NID, Y, T_{i4}, T_{s3}, V_5\} \Longrightarrow$	$SK_{ij} = h(h(x) \Vert h'(y) \Vert Ac'_j \Vert T_{i4})$
...	$X = h(x) \oplus h(Ac'_j \Vert T_j)$
$5) \lvert T_j - T_{i4} \rvert < \triangle t \quad M_8: \Longleftarrow$	$V_6 = E_{SK}(ID_j, h'(y), T_j)$
$h'(x) = X \oplus h(Ac_j \Vert T_j)$	$\Longleftarrow M_8: \{TID_j, V_6, X, T_j\}$
$SK'_{ij} = h(h'(x) \Vert h(y) \Vert Ac'_j \Vert T_{i4})$	$Store: TID_j$
$\{ID_j, T_j, h'(y)\} = D_{SK}(V_6)$	
$h'(y) =?\ h(y)$	
$Store: TID_j, ID_j$	

Figure 5: IotC_i offline access to WS_j node.

4.6. IotC Accesses Multiple WS Nodes Concurrently. In a multi-WS access scenario, Figure 5 shows that the variable Ac_j in the authorization process is an array AC [1, . . ., N]. AC [1, . . ., N] contains the access verification codes for multiple WS nodes. At this time, IotC generates a corresponding message TID and message M_7 for each element in AC [1, . . ., N], according to the operation described in Figure 5. The messages of multiple M_7 structures were then sent continuously.

After WS_j receives the first M_7 structure message, WS_j starts to execute all operations in the "(3)" mark section in Figure 5. Until $V_5 = ?h(\mathrm{TID}_j \Vert \mathrm{NID} \Vert Ac'_j \Vert T_{s3} \Vert T_{i4} \Vert h'(y))$ meets the equality, stop receiving and go to the part marked with "(4)."

In the case of multiple WS concurrent access, after IotC_i receives M_8, IotC_i uses the TID in M_8 to select the corresponding AC to improve the concurrent access capability of IotC_i.

4.7. Replacement and Change of WS Nodes. When the patient's condition development or other conditions need to adjust the IotC, this can be realized by sequentially executing the process described in Figures 4 and 5. When only the WS needs to be adjusted, this can be realized by sequentially executing the process described in Figures 4 and 5.

5. Security Analysis

This section proves the security performance and antiattack ability of the proposed protocol through formal methods.

5.1. Security Model. The scheme proposed in this study belongs to the identity authentication and key agreement (AKA) protocol. Therefore, we provide the corresponding security model and formal proof process based on [31–33]. In this model, $\mathbb{P}$ denotes the proposed scheme. I presents the participants in the scheme, which can be TA, $IotC_i$, or WS_j. Attacker $\mathscr{A}$ can be described by the following random oracles:

(i) Excute$(TA, \mathrm{IotC}_i, WS_j)$: attacker $\mathscr{A}$ intercepts all messages exchanged between any two parties

(ii) Send(I, m): attacker $\mathscr{A}$ sends forged message M to I and receives feedback form

(iii) Reveal(I): attacker $\mathscr{A}$ obtains the composition information of the session key and launches a known key attack

(iv) Corrupt(I): attacker $\mathscr{A}$ can obtain the long-term key of I to verify the strong forward security performance of the session key SK

  (i) Corrupt(IotC): attacker $\mathscr{A}$ can obtain $\{ID_i, TC_i,\}$ of IotC

  (ii) Corrupt(WS): attacker $\mathscr{A}$ can obtain $\{ID_j, TC_j\}$ of WS

(v) Test(I): Attacker $\mathscr{A}$ uses a coin toss test to challenge session key {SK}. When $\rho = 1$, the correct session key SK is returned, and when $\rho = 0$, a random string is returned.

(vi) Hash$(m, h(m))$: Attacker $\mathscr{A}$ calculates the hash value of message M.

Definitions and assumptions need to be used in the definition and false proof process.

5.1.1. Partnering. If a group of participants in the protocol, the instances of IotC_i and WS_j, can pass the mutual identity authentication and negotiate a consistent session key SK, we call them partners.

5.1.2. Fresh. If a session is not disclosed, it is called a fresh session.

5.1.3. Security. When attacker $\mathscr{A}$ destroys the security advantage $\mathrm{Adv}_p(\mathscr{A}) \le \varepsilon$ of protocol $\mathbb{P}$, it means that $\mathbb{P}$ is secure and satisfies $\mathrm{Adv}_p(\mathscr{A}) = |2\,\mathrm{Pr}\,[\mathrm{Succ}] - 1|$, where ε is a real number small enough to be ignored, and Pr [Succ] represents the probability that attacker $\mathscr{A}$ successfully destroys the security of $\mathbb{P}$.

Assumptions 1. The basic algorithms used in the proposed scheme, such as the elliptic curve discrete logarithm problem (ECDLP), elliptic curve Diffie–Hellman discrete logarithm problem (ECDHDLP), fuzzy extractor (FE), hash function, and symmetric-key encryption algorithm (Enc), are secure; that is,$\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}) \leq \varepsilon$, $\mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A}) \quad \leq \varepsilon$, $\mathrm{Adv}_{FE}(\mathscr{A}) \leq \varepsilon$, $\mathrm{Adv}_{\mathrm{HASH}}(\mathscr{A}) \leq \varepsilon$, $\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A}) \leq \varepsilon$.

5.2. Security Proof

Theorem 1. *The advantage of $\mathscr{A}$ in $\mathbb{P}$ is given by*

$$\begin{aligned}\mathrm{Adv}_p(\mathscr{A}) \leq 2\frac{q_h^2}{2^l} + 22\frac{(q_h + q_s)}{2^l} + 4\frac{(q_s + 2T_m)}{2^q} + 2\frac{q_s}{|\mathfrak{H}|}\\ + 2\frac{q_h^4}{2^{2l+2}} + 2\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A}) + \frac{q_h^2}{2^l}\\ \max\{\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A})\}.\end{aligned} \tag{1}$$

In the above formula, q is the order of elliptic curve finite cyclic group $E(F_p)$; $|\mathfrak{H}|$ represents the length of the dictionary; l is the length of the hash value, q_e, q_s,and q_h, respectively, represent the number of times $\mathscr{A}$ executes Excute(), Send(), and Hash() queries, respectively, and T_m represents the calculation times of elliptic curve scalar multiplication.

Proof. This process is similar to those in References [31–33] and takes place over five games G_0 to G_7. Succ_i represents that $\mathscr{A}$ wins in the game G_i and successfully destroys the security of protocol $\mathbb{P}$.

G_0: This game simulates that attacker $\mathscr{A}$ uses the random oracle model to launch a real attack on $\mathbb{P}$, so we can obtain $\mathrm{Adv}_p(\mathscr{A}) = |2\,\mathrm{Pr}\,[\mathrm{Succ}_0] - 1|$.

G_1: This game simulates attacker $\mathscr{A}$ launching a passive attack on protocol $\mathbb{P}$. Attacker $\mathscr{A}$ intercepts message $\mathrm{M}_3 - M_8$ through $\mathrm{Excute}(TA, \mathrm{Iot}C_i, WS_j)$ and stores it in the list L. Because the key SK is not transmitted in the above message, passive attacks will not increase the advantage of attacker $\mathscr{A}$. Thus, $\mathscr{A}$ can be obtained $\mathrm{Pr}[\mathrm{Succ}_1] = \mathrm{Pr}[\mathrm{Succ}_0]$.

G_2: To improve the advantage, attacker $\mathscr{A}$ applies the collision principle based on G_1 and uses an oracle $\mathrm{Hash}(m, h(m))$ and $\mathrm{Test}(I)$ to launch multiple attacks. In this case, attacker $\mathscr{A}$ guesses or collides with the key SK, and the success probability is $q_s/|\mathfrak{H}| + q_h^2/2^{l+1}$; destroying the security of the symmetric-key algorithm, and the success probability is $\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A})$. At this point, the advantage of attacker $\mathscr{A}$ can be described as $\mathrm{Pr}[\mathrm{Succ}_2] - \mathrm{Pr}[\mathrm{Succ}_1] \leq q_s/|\mathfrak{H}| + q_h^2/2^{l+1} + \mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A})$.

G_3: Attacker $\mathscr{A}$ indirectly attacks SK through Ac_j based on G_2: Attacker A can destroy the security of the symmetric-key algorithm. The methods and success probability of attacker $\mathscr{A}$ are as follows:

(i) Attacker $\mathscr{A}$ collides with the value of Ac_j, and the success probability is $q_h^2/2^{l+1}$.

(ii) Attacker $\mathscr{A}$ intercepts NID and T_{s3} in M_7, collides with ID_j and TC_j values, and uses the formula $Ac_j = h(NID\Big\|ID_j\|TC_j\|T_{s3})$ to calculate Ac_j, with a success probability of $q_h^4/2^{2l+2}$.

(iii) Attacker $\mathscr{A}$ uses the formula $Ac_j = E_j \oplus h(\mathrm{Q}\|\mathrm{PTC}\|T_{s3})$ to calculate the value of Ac_j, where Q and PTC are unknown variables, and the success probability is $\max\{\mathrm{Adv}_{\mathrm{ECDLP}}\ (\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}\ (\mathscr{A})\}q_h^2/2^{l+1}$.

At this point, the advantage of attacker $\mathscr{A}$ can be described as $\mathrm{Pr}[\mathrm{Succ}_3] - \mathrm{Pr}[\mathrm{Succ}_2] \leq q_h^2\ /2^{l+1} + q_h^4/2^{2l+2} + \max\{\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}\ (\mathscr{A})\}q_h^2/2^{l+1}$.

G_4: This game simulates that attacker $\mathscr{A}$ uses $\mathrm{Send}(\mathrm{Iot}C_i, M_8)$ query to send a forged message M_8 to enhance his advantage. In this case, attacker $\mathscr{A}$ evaluates the success according to the message returned by $\mathrm{Iot}C_i$. The simulator must check whether M_8 is in the list L. To verify the formula $h'(y) = ?h(y)$, attacker $\mathscr{A}$ must test the values of $h(x)$, Ac_j', and SK'_{ij}. Therefore, attacker $\mathscr{A}$ can obtain $\mathrm{Pr}[\mathrm{Succ}_4] - \mathrm{Pr}\ [\mathrm{Succ}_5] \leq 3(q_h + q_s)/2^l$.

G_5: This game simulates that attacker $\mathscr{A}$ uses $\mathit{Send}(WS_j, M_7)$ query to send a forged message M_7 to enhance its advantage. In this case, attacker $\mathscr{A}$ passes the formula $V_5 = ?h(TID_j\Big\|NID\|Ac_j'\|T_{s3}\|T_{i4}\|h'(y))$ for verification, and the values of $h(y)$, Ac_j', TC_j, and ID_j need to be tested. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_5] - \mathrm{Pr}[\mathrm{Succ}_4] \leq 4(q_h + q_s)/2^l$.

G_6: This game simulates that attacker $\mathscr{A}$ uses $\mathit{Send}(\mathit{Iot}C_i, M_6)$ query to send a forged message M_6 to enhance his advantage. In this case, attacker $\mathscr{A}$ must test the values of Q', PID, and PTC. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_5] - \mathrm{Pr}[\mathrm{Succ}_4] \leq (\mathrm{q_s} + 2\mathrm{T_m})/2^{\mathrm{q}} + 2(q_h + q_s)/2^l$.

G_7: This game simulates that attacker $\mathscr{A}$ uses $\mathrm{Send}(TA, M_5)$ queries to send a forged message M_5 to enhance its advantage. In this case, attacker $\mathscr{A}$ must test the values of B, PID, and PTC. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_6] - \mathrm{Pr}[\mathrm{Succ}_5] \leq (\mathrm{q_s} + 2\mathrm{T_m})/2^{\mathrm{q}} + 2(q_h + q_s)/2^l$.

Therefore, combining the advantages of G_0–G_7 attacker $\mathscr{A}$, we can get Theorem 1. □

5.3. BAN Logic Proof of the Proposed Protocol. In this chapter, we use the Burrows–Abadi–Needham (BAN) logic [30, 34, 35] to formally prove the security of the device AKA protocol proposed in this study. We assumed that the symbols P and Q represent participation in the communication session, X and Y are messages sent or received by the participants, and K is the session key. Table 2 lists the relevant symbols, descriptions, and logic rules often used in the BAN logic. To save space, only Figure 5 is listed as a formal proof describing the content.

Table 2: BAN logic notation and rules.

$P\mid\equiv X$	P believes the message X
$P\triangleleft X$	P sees the message X
$P\mid\sim X$	P once said the message X
$P\mid\Rightarrow X$	P has jurisdiction over the message X
$\#(X)$	The message X is fresh
$P\overset{Y}{\rightleftharpoons}YQ$	Only P and Q know X
$P\overset{K}{\leftrightarrow}Q$	P and Q share key K
(X,Y)	X or Y is a part of message (X, Y)
$\{X_K$	X is encrypted with K
$(X)_K$	X is hashed with K
R1	Message meaning rule: $(\mathrm{P}\mid\equiv\mathrm{P}\overset{\mathrm{K}}{\leftrightarrow}\mathrm{Q},\mathrm{P}\triangleleft\mathrm{X_K}/\mathrm{P}\mid\equiv\mathrm{Q}\mid\sim\mathrm{X})$, $(\mathrm{P}\mid\equiv\mathrm{P}\overset{\mathrm{Y}}{\rightleftharpoons}\mathrm{YQ},\mathrm{P}\triangleleft\{\mathrm{X_Y}/\mathrm{P}\mid\equiv\mathrm{Q}\mid\sim\mathrm{X})$
R2	Nonce verification rule: $(\mathrm{P}\mid\equiv\#(\mathrm{X}),\mathrm{P}\mid\equiv\mathrm{Q}\mid\sim\mathrm{X}/\mathrm{P}\mid\equiv\mathrm{Q}\mid\equiv\mathrm{X})$
R3	Jurisdiction rule: $(\mathrm{P}\mid\equiv\mathrm{Q}\mid\Rightarrow\mathrm{X},\mathrm{P}\mid\equiv\mathrm{Q}\mid\equiv\mathrm{X}/\mathrm{P}\mid\equiv\mathrm{X})$
R4	Freshness rule: $(\mathrm{P}\mid\equiv\#(\mathrm{X})/\mathrm{P}\mid\equiv\#(\mathrm{X},\mathrm{Y}))$,
R5	Belief rule: $(\mathrm{P}\mid\equiv\mathrm{X},\mathrm{P}\mid\equiv\mathrm{Y}/\mathrm{P}\mid\equiv(\mathrm{X},\mathrm{Y}))$, $(\mathrm{P}\mid\equiv(\mathrm{X},\mathrm{Y})/\mathrm{P}\mid\equiv\mathrm{X})$, $(\mathrm{P}\mid\equiv\mathrm{Q}\mid\equiv(\mathrm{X},\mathrm{Y})/\mathrm{P}\mid\equiv\mathrm{Q}\mid\equiv\mathrm{X})$

According to the functional characteristics of the protocol proposed in this study, the security of the AKA process of IotC_i accessing WS_j can be decomposed into five security verification objectives under the BAN logic. They are, respectively, G1: WS_j trust TA, G2: WS_j trust IotC_i, G3: WS_j trust SK_{ij}, G4: IotC_i trust SK_{ij}, and G5: IotC_i trust WS_j.

5.3.1. *G1: WS_j Authenticates TA.*

In BAN logic, the message M_7: $\{\mathrm{TID}_j,\mathrm{NID},Y,T_{i4},T_{s3},V_5\}$ in Figure 5 is converted to $(\mathrm{TID}_j,\mathrm{NID},T_{i4},T_{s3},Y,T_{i4ACj},(\mathrm{TI\ D}_j,\mathrm{NID},T_{s3},T_{i4},Y)_{ACj})$. After receiving M_7, WS_j calculates $AC_j'=(\mathrm{NID},ID,T_{s3})_{TCj}$, and the target G1 can be represented by the formula $WS_j\mid\equiv TA\mid\sim AC_j'$. When the equation $V_5=?h(\mathrm{TID}_j\|\mathrm{NID}\|AC_j'\|T_{s3}\|T_{i4}\|Y)$ holds, AC_j is not tampered with.

WS_j gets $WS_j\mid\equiv TA\overset{TC_j}{\longleftrightarrow}WS_j,W\quad S_j\mid\equiv TA\mid\equiv TA\overset{TC_j}{\longleftrightarrow}C_jW\ S_j,WS_j\triangleleft(\mathrm{NID},ID_j,T_{s3})_{TCj}$

Uses R1: $(WS_j\mid\equiv TA\overset{TC_j}{\rightleftharpoons}WS_j,W\ S_j\triangleleft(\mathrm{NID}\ ,ID,T_{S3})_{TC_j}/WS_j\mid\equiv TA\mid\sim(NID,ID,T_{S3})_{TC_j})$

Gets G1: $WS_j\mid\equiv TA\mid\sim AC_j'$

5.3.2. *G2: WS_j Trust* IotC_i.

In the protocol proposed in this study, IotC_i uses NID to mark the identity after binding with patient information and obtaining WS access authorization. Therefore, the target G2 can be represented by the formula $WS_j\mid\equiv\mathrm{NID}$.

WS_j gets $WS_j\mid\equiv TA\overset{TC_j}{\longleftrightarrow}WS_j$, $WS_j\mid\equiv\#T_{s3}$, $WS_j\mid\equiv TA\mid\Rightarrow(\mathrm{NID},\mathrm{IDj},T_{S3})_{TC_j}$

Uses R4: $(WS_j\mid\equiv\#T_{s3}/WS_j\mid\equiv\#(\mathrm{NID},ID,T_{S3})_{TC_j})$

Uses R2: $(WS_j\mid\equiv\#(\mathrm{NID},ID,T_{S3})_{TC_j},WS_j\mid\equiv TA\mid\sim\mathrm{NID},ID,T_{S3})_{TC_j}\ /WS_j\mid\equiv TA\mid\equiv(\mathrm{NID},ID,T_{S3})_{TC_j})$

Uses R3: $(WS_j\mid\equiv TA\mid\Rightarrow(\mathrm{NID},ID,T_{S3}\ )_{TC_j},WS_j\mid\equiv TA\mid\equiv\mathrm{NID},ID,T_{S3})_{TC_j}/WS_j\mid\equiv(\mathrm{NID},ID,T_{S3})_{TC_j})$

Uses R5: $(WS_j\mid\equiv(\mathrm{NID},ID,T_{S3})_{TC_j}\ /WS_j\mid\equiv\mathrm{NID},WS_j\mid\equiv ID_j,WS_j\mid\equiv T_{S3})$

Gets G2: $WS_j\mid\equiv\mathrm{NID}$

5.3.3. *G3: WS_j Trusts SK_{ij}.*

SK_{ij} is calculated using the formula $SK_{ij}=h(h(x)\|h(y))$, and its calculation security is based on a collision-resistant hash function. $h(x)$ is randomly generated by WS_j. G3 can be expressed using the formula $WS_j\mid\equiv h(y)$.

WS_j gets $WS_j\mid\equiv\#T_{i4}$, $WS_j\triangleleft h(y),T_{i4ACj}$, $WS_j\mid\equiv TA\mid\Rightarrow h(y),T_{i4ACj}$

Uses R1: $(WS_j\mid\equiv WS_j\overset{AC_j}{\rightleftharpoons}TA,WS_j\ \triangleleft h(y),T_{i4AC_j}/WS_j\mid\equiv TA\mid\sim\ (h(y),T_{i4}))$

Uses R2: $(WS_j\mid\equiv\#T_{i4},WS_j\mid\equiv TA\mid\sim(h(y),T_{i4})/WS_j\mid\equiv TA\mid\equiv(h(y),T_{i4}))$

Uses R3: $(WS_j\mid\equiv TA\mid\Rightarrow h(y),T_{i4AC_j},WS_j\mid\equiv TA\mid\equiv(h(y),T_{i4})/WS_j\mid\equiv(h(y),T_{i4}))$

Uses R5: $(WS_j\mid\equiv(h(y),T_{i4})/WS_j\mid\equiv h(y),WS_j\mid\equiv T_{i4})$

Gets G3: $WS_j\mid\equiv h(y)$

5.3.4. *G4:* IotC_i *Trusts SK_{ij}.*

In BAN logic, message M_8 is converted to $(\mathrm{TID}_j,ID_j,Y',T_{jSK_{ij}},X,T_{jAC_j},T_j)$. G4 can be represented using the formula Iot$C_i\mid\equiv SK_{ij}$.

IotC_i gets Iot$C_i\mid\equiv Ac_j$, Iot$C_i\mid\equiv$ Iot $C_i\overset{AC_j}{\rightleftharpoons}TA$, Iot$C_i\triangleleft h(x),T_j\}_{Ac_j}$, Iot$C_i\mid\equiv h(y)$

Uses R1: (Iot$C_i\mid\equiv$ Iot$C_i\overset{AC_j}{\rightleftharpoons}TID$, Iot$C_i\triangleleft h(x),T_j\}_{Ac_j}/$ Iot$C_i\mid\equiv TID\mid\sim(h(x),T_j)$)

Uses R4: (Iot$C_i\mid\equiv\#(T_j)/$Iot$C_i\mid\equiv\#(h(x),T_j)$)

Uses R2: (Iot$C_i\mid\equiv\#(h(x),T_j)$, Iot$C_i\mid\equiv TID\mid\sim(h(x),T_j)/WS_j\mid\equiv\mathrm{NID}\mid\equiv(h(x),T_j)$)

Uses R3: (Iot$C_i\mid\equiv TA\mid\Rightarrow$Iot$C_i\ \overset{AC_j}{\rightleftharpoons}TA$, Iot$C_i\mid\equiv\mathrm{NID}\mid\equiv(h(x),T_j)/IotC_i\mid\equiv(h(x),T_j)$)

Uses R5: $(\text{Iot}C_i \mid \equiv (h(x), T_j)/\text{Iot}C_i \mid \equiv h(x))$, $(\text{Iot}C_i \mid \equiv h(x), \text{Iot}C_i \mid \equiv h(y)/\text{Iot}C_i$
$\mid \equiv (h(x), h(y)))$

Gets G4: Uses $\text{Iot}C_i \mid \equiv SK'_{ij}$

5.3.5. G5: $\text{Iot}C_i$ *Trusts* WS_j. G4 can be represented by the following formula $\text{Iot}C_i \mid \equiv ID_j$:

Uses R1: $(\text{Iot}C_i \mid \equiv \text{Iot}C_i \overset{SK_{ij}}{\rightleftharpoons} \text{TID}, \text{Iot}C_i \lhd \text{I}D_j, \text{h}'(\text{y}), T_j\}_{SK_{ij}}/\text{IoT}C_i \mid \equiv T\text{ID} \mid \sim (\text{I}D_j, \text{h}'(\text{y}), T_j))$

Uses R4: $(\text{Iot}C_i \mid \equiv \#(T_j)/\text{Iot}C_i \mid \equiv \#(\text{I}D_j, \text{h}'(\text{y}), T_j))$

Uses R2: $(\text{Iot}C_i \mid \equiv \#(\text{I}D_j, \text{h}'(\text{y}), T_j)$, $\text{Iot}C_i \mid \equiv \text{TID} \mid \sim (\text{I}D_j, \text{h}'(\text{y}), T_j)$ $/\text{Iot}C_i \mid \equiv \text{TID} \mid \equiv (\text{I}D_j,\ \text{h}'(\text{y}), T_j))$

Uses R3: $(\text{Iot}C_i \mid \equiv \text{TID} \mid \Rightarrow \text{Iot}C_i \overset{SK_{ij}}{\rightleftharpoons} \text{TID}, \text{Iot}\ \ C_i \mid \equiv \text{TID} \mid \equiv (\text{I}D_j, \text{h}'(\text{y}), T_j)/\text{Iot}C_i \mid \equiv (\text{I}D_j,\ \text{h}'(\text{y}), T_j))$

Uses R5: $(\text{Iot}C_i \mid \equiv (\text{I}D_j, \text{h}'(\text{y}), T_j)/\text{Iot}C_i \mid \equiv \text{I}\ D_j, \text{Iot}\ C_i \mid \equiv \text{h}'(\text{y}), \text{Iot}C_i \mid \equiv T_j)$

Gets G5: $\text{Iot}C_i \mid \equiv \text{I}D_j$

At this time, this study successfully uses the BAN logic to formally prove the security of the three-party AKA protocol proposed in this study and achieves all the security indicators.

6. Simulation of the Proposed Protocol

AVISPA [25, 36, 37] is an automated network protocol security verification tool. It includes a constraint-logic attacker search (Cl-AtSe) and an on-the-fly model checker (OFMC), which are two types of network attack simulation checkers. The results of AVISPA evaluation showed a certain degree of recognition. In this part, this study uses the AVISPA tool set for Figure 4 authorized access and equipment AKA process described in Figure 5 and conduct simulation security verification.

Figure 6 shows the HLPSL simulation model of the proposed protocol and the simulation attack process in the AVISPA software. Attacker A was added to the simulation process to verify the ability of the protocol to resist intermediate authentication attacks. Figure 7 evaluates the results of the HLPSL model in AVISPA software using two checkers: OFMC and Cl-AtSe. The results show that the proposed scheme is secure under the two inspector models and meets all specified security objectives.

7. Efficiency Evaluation and Comparisons

In this section, the requirements of computing resources and server I/O resources that have a significant impact on system stability are selected, and the lightweight three-party AKA scheme proposed in this study is evaluated. For convenience of description, we select the typical [5–7, 9, 23, 26] lightweight authentication and key agreement protocols in some recent studies for comparison.

7.1. Comparison of the Computation Cost. When the encryption algorithm is fixed, the higher the security level, the longer the key length, and more computing resources are required to be consumed [28]. An objective analysis of the resource consumption of the AKA scheme must be conducted at the same security level. Therefore, Table 3 is established by referring to the relevant experimental data and the results in references [6, 9, 23, 38, 39].

Table 3 lists the approximate time multiple relationships between the main mathematical calculation in some common security encryption algorithms and the SHA-1 hash calculation, and the unit is T_h. For the special T_{fe}, we have not yet found convincing public data; T_{xor} takes very little time and can be ignored.

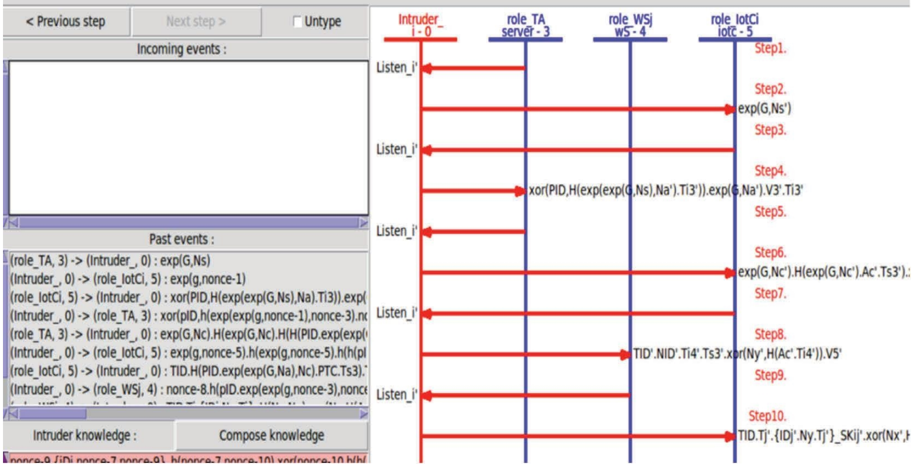
Table 4 compares the selected literature and the proposed AKA scheme in terms of the theoretical consumption of resources. Considering that IotC in the proposed scheme can support offline and concurrent access to multiple WS nodes within the authorization time range, the corresponding computing resource consumption is listed in Table 4.

In the case of online access, the proposed protocols IotC and TA must perform the authorization process described in Figure 4. Therefore, when accessing the first WS node, the TA must perform three EC scalar multiplications and six hash calculations, that is, $2T_{sm} + 6T_h \approx 151T_h$ calculation time, IotC requires $1T_{fe}$+ 3 $T_{sm} + 13T_h + 3T_{\text{sym}} \approx 233.5T_h + 1T_{fe}$ calculation time, and WS requires $5T_h + 1T_{\text{sym}} \approx 6\text{T}_\text{h}$ calculation time. When the IotC offline line accesses the second WS node, the proposed scheme no longer needs to perform the authorization process described in Figure 4. Currently, IotC requires only a calculation time of $5T_h + 1T_{\text{sym}} \approx 6T_h$, whereas WS requires a calculation time of $5T_h + 1T_{\text{sym}} \approx 6T_h$.

Figure 8 shows a comparison of the schemes in Table 4 when only one WS node needs to be accessed. The x-axis represents the theoretically calculated resource demand quantity, and the unit is T_h. The computational performance of Li et al. [9] scheme is the best, and the proposed scheme has certain advantages.

Figure 9 shows the proposed scheme and compares the demand for computing resources with the protocol proposed by Jiang et al. [26] for multi-WS node access. The x-axis represents the number of access WS nodes, and the y-axis represents the theoretically calculated resource demand in units of T_h. Figure 9(a) describes the changes in the computing resource requirements of IotC. Figure 9(b) represents the change in computing resource demand of server TA. Figure 9(c) describes the change in overall computing resources. The increase in the number of nodes has little impact on IotC and the overall computing resource requirements in the scheme proposed in this study, which is better than Jiang's scheme.

7.2. Server Database I/O Resources. The number of WS, IotCs, and users in an IoHT system is huge, and the necessary information needs to be stored in the database. When



```
(role_TA, 3) -> (Intruder_, 0) : exp(G,Ns)
(Intruder_, 0) -> (role_IotCi, 5) : exp(g,nonce-1)
(role_IotCi, 5) -> (Intruder_, 0) : xor(PID,H(exp(exp(G,Ns),Na).Ti3)).exp(
(Intruder_, 0) -> (role_TA, 3) : xor(pID,h(exp(exp(g,nonce-1),nonce-3).nc
(role_TA, 3) -> (Intruder_, 0) : exp(G,Nc).H(exp(G,Nc).H(H(PID.exp(exp(
(Intruder_, 0) -> (role_IotCi, 5) : exp(g,nonce-5).h(exp(g,nonce-5).h(h(pI
(role_IotCi, 5) -> (Intruder_, 0) : TID.H(PID.exp(exp(G,Na),Nc).PTC.Ts3).
(Intruder_, 0) -> (role_WSj, 4) : nonce-8.h(pID.exp(exp(g,nonce-3),nonce
```

```
nonce-9.{iDj.nonce-7.nonce-9}_h(nonce-7.nonce-10).xor(nonce-10.h(h(
```

Figure 6: Simulation attack process of the proposed protocol.

```
% OFMC
% Version of 2006/02/13
   SAFE
DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
   /home/span/span/testsuite/results/3AKA2-12.1.if
GOAL
   as_specified
BACKEND
   OFMC
COMMENTS
STATISTICS
   parseTime: 0.00s
   searchTime: 0.01s
   visitedNodes: 5 nodes
   depth: 4 plies
```

(a)

```
SUMMARY
   SAFE
DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
   TYPED_MODEL
   BOUNDED_SEARCH_DEPTH
PROTOCOL
   /home/span/span/testsuite/results/3AKA2-12.1.if
GOAL
   As Specified
BACKEND
   CL-AtSe
STATISTICS
   Analysed : 5 states
   Reachable : 2 states
   Translation: 0.01 seconds
   Computation: 0.00 seconds
```

(b)

Figure 7: (a) OFMC report. (b) Cl-AtSe report.

Table 3: Time requirement of the calculation method.

Signs	Description	Times (T_h)
T_h	Hash function	= 1
T_{sym}	Symmetric encryption/decryption	≈1
T_{MAC}	Message authentication code	≈1
T_{pa}	EC point addition	≈12.5
T_{crt}	Chinese remainder theorem (CRT)	≈20
T_{me}	Modular exponentiation	≈60
T_{sm}	EC scalar multiplication	≈72.5
T_{sig}	Signature generation using ECDSA	≈92.5
T_{Ver}	Signature verification using ECDSA	≈147.5
T_{map}	Map-to-point on ECC	≈450
T_{pair}	ECC bilinear pairing	≈1500
T_{fe}	Fuzzy extractor function	—
T_{xor}	Time required for XOR operation	Negligible

Table 4: Comparison of calculated resource consumption.

Protocol	Server	SGW/IoetC/HN	STD/node	Total
Das et al. [5]	—	$10\ T_h + 1T_{fe}$	$7\ T_h$	$17\ T_h + 1\ T_{fe}$
Srinivas et al. [6]	$11T_h + 1T_{\text{ctr}}$	$16T_h + 1T_{\text{me}}$	$12T_h$	$118T_h$
Wang et al. [7]	$377\ T_h$	$75.5\ T_h$	$163.5\ T_h$	$661\ T_h$
Li et al. [9]	—	$5T_h$	$3T_h$	$8\ T_h$
He and Zeadally [23]	$77.5\ T_h$	$221.5\ T_h$	$149.5\ T_h$	$448.5\ T_h$
Jiang et al. [26]	$9T_h + 1sm$	$8T_h + 2T_{sm} + 1T_{fe}$	$4\ T_h$	$239.5\ T_h + 1T_{fe}$
Ours online, 1st node	$2\ T_{sm} + 6\ T_h \approx\ 151\ T_h$	$3\ T_{sm} + 13\ T_h + 3\ T_{\text{sym}} \approx\ 233.5\ T_h + 1T_{fe}$	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$390.5\ T_h + 1\ T_{fe}$
Ours online, 2nd node	$1T_h$	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$13T_h$
Ours offline, 1st node	0	$8\ T_h + 2\ T_{\text{sym}} + 1T_{fe} \approx\ 10\ T_h + 1T_{fe}$	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$16\ T_h + 1T_{fe}$
Ours offline, 1st node	0	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$5\ T_h + 1\ T_{\text{sym}} \approx\ 6\ T_h$	$12T_h$

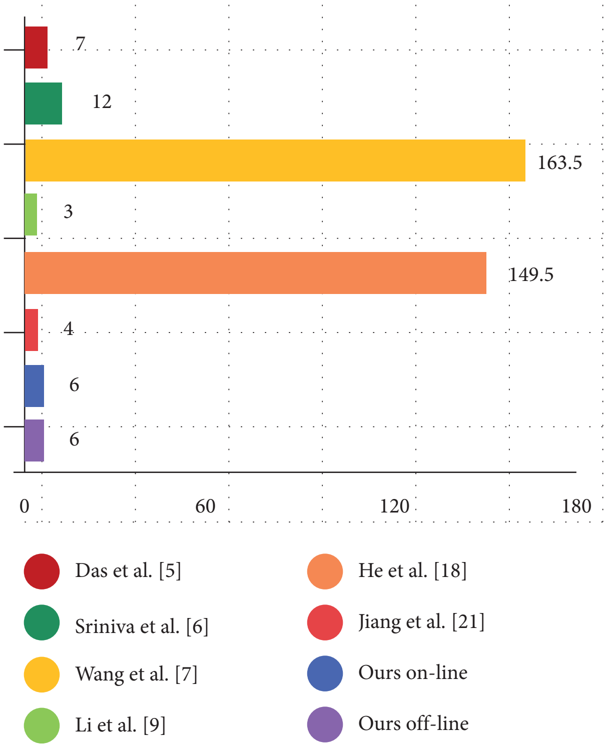
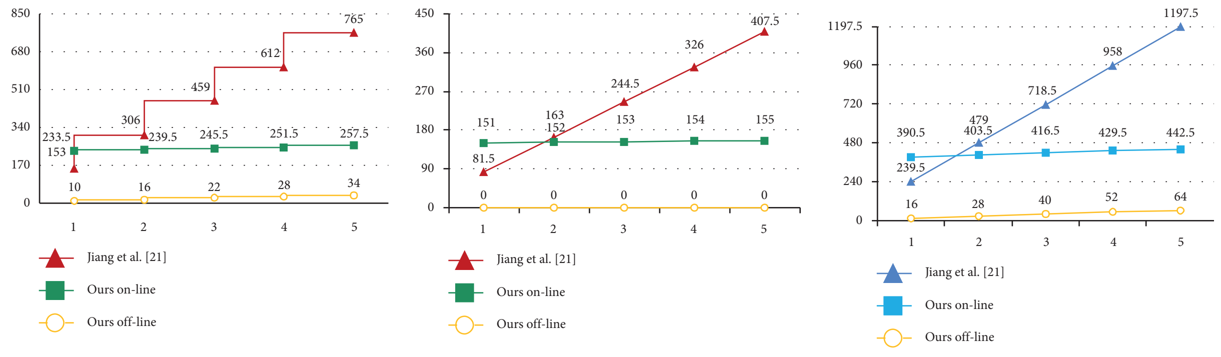


Figure 8: WS calculation time.



(a) (b) (c)

Figure 9: Computing resource requirements when multiple WS nodes are connected.

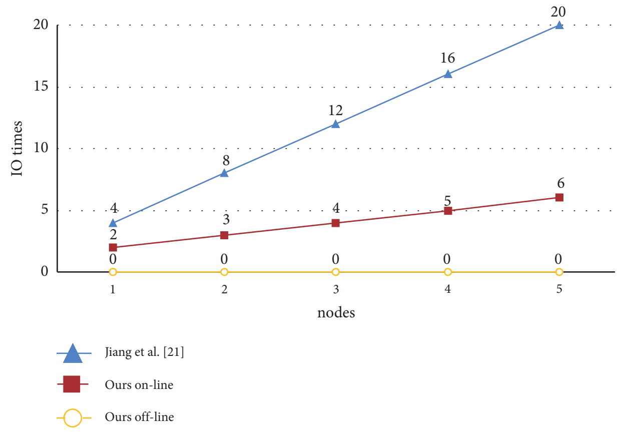


FIGURE 10: Comparison of server database I/O operations.

IotC is connected to WS, TA must perform the necessary data reading or writing operations to verify the privileges of users after IotC binding and authorize IotC to access the specified WS. The operation of the database requires server I/O resources. This operation is too frequent, which causes insufficient input-output resources and seriously affects the stability of the system.

In Jiang et al.'s scheme [26], privacy protection is realized and device tracking is prevented by synchronizing a set of one-time identity IDs between the WS and server CS. Thus, Ta must perform three queries and one updated data operation during the AKA process. Specifically, an IotC identity query, a temporary ID query of WS, avoids the repeated query of the one-time ID of the newly generated WS at one time and an operation to update the database with a new ID. The proposed scheme requires only one PID query and WS information query. Moreover, when the number of WS nodes increases, the number of queries must be increased to be equal to the number of authorized WS nodes. Figure 10 shows the changes in the I/O operation resource requirements of the server TA database in the case of multi-WS access in the proposed scheme and Jiang et al.'s scheme [26].

8. Conclusions

The rapid development of the Internet of Things and wearable sensing technology has continuously promoted Internet of Health Things (IoHT) systems in medical institutions. However, the IoHT systems not only provide a more convenient and faster channel for health detection data but also make sensitive Personal Health Information (PHI) face many new security risks. Physical channel security between Internet of Things Connectors (IotC) and wearable sensors (WS) is an important link for building IoHT systems into a secure health system (SHS).

Therefore, this study proposes a lightweight three-party authentication and key agreement (AKA) protocol that meets the characteristics of the two-hop structure and the requirements of multi-WS network monitoring. The results of the formal security proof, BAN logic analysis, and simulation experiment of the AVISPA tools show that the scheme proposed in this study can meet the expected security requirements. The results of the comparison with relevant protocols show that the protocol has certain advantages in WS individual computing resource consumption: in the scenario of multiple WS node applications, the increasing trend of computing resource demand of IotC and the server is not obvious, as the I/O operation resources of the server are not affected by the number of WS nodes.

Acronyms

AVISPA:	Automated validation of internet security protocols and applications
AKA:	Authentication and key agreement
BAN logic:	Burrows–Abadi–Needham logic
CS:	Cloud server
Cl-AtSe:	Constraint-logic attacker search
DOS:	Denial-of-service
EC:	Elliptic curve
ECC:	Elliptic curve cryptography
ECDLP:	Elliptic curve discrete logarithm problem
ECDHDLP:	Elliptic curve Diffie–Hellman discrete logarithm problem
FE:	Fuzzy extractor
IoT:	Internet of Things
IoHT:	Internet of Health Things
IotC:	Internet of things Connector
IoD:	Internet of Drones
I/O:	Input/Output
MT:	Mobile terminal
OFMC:	On-the-fly model checker
PHI:	Patient health information
SHS:	Secure health system
TA:	Third-party authentication server
WS:	Wearable sensor
WNC:	Wearable network connector.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Science and Technology Research Project of Hebei Province Colleges and Universities (Grant Z2020134) and the Natural Science Foundation of Hebei Province (Grant F2021405001) and the General Project of Hebei North University under Grant no. XJ2021005.

References

[1] researchandmarkets, "Wearable technology market by product (wristwear, headwear, footwear, fashion & jewelry, bodywear), type (smart textile, non-textile), application (consumer electronics, healthcare, enterprise & industrial), and geography - global forecast to 2026," 2021, https://www.

researchandmarkets.com/reports/5314641/wearable-technology-market-by-product-wristwear.

[2] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[3] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, p. 768, 2019.

[4] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, 2020.

[5] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, J, 2018.

[6] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 942–956, 2020.

[7] Z. Wang, L. Gong, J. Yang, and X. Zhang, "Cloud-assisted elliptic curve password authenticated key exchange protocol for wearable healthcare monitoring system," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 9, 2020.

[8] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, p. 117, 2016.

[9] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[10] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3618–3627, 2018.

[11] A. K. Yetisen, J. L. Martinez-Hurtado, B. Ünal, A. Khademhosseini, and H. Butt, "Wearables in medicine," *Advances in Materials*, vol. 30, no. 33, Article ID 1706910, 2018.

[12] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[13] P. A. H. Williams and V. McCauley, *Always Connected: The Security Challenges of the Healthcare Internet of Things*, IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 2016.

[14] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: blockchain-based telesurgery framework for healthcare 4.0," in *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Beijing, China, August 2019.

[15] P. A. Abdalla and C. Varol, "Testing IoT security," *The Case Study of an IP Camera*, vol. 8, 2020.

[16] X. Zhang, J. Zhao, F. Yang, Q. Zhang, and X. Zhang, "An automated composite scanning tool with multiple vulnerabilities," in *Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China, October 2019.

[17] Z. Mu, W. Li, C. Lou, and M. Liu, "Investigation and application of smart door locks based on bluetooth control technology," in *Proceedings of the 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, Dalian, China, April 2020.

[18] C. Doctorow, "Proof-of-concept ransomware for smart thermostats demoed at defcon," Boing Boing, 2016, https://boingboing.net/2016/08/08/proof-of-concept-ransomware-fo.html.

[19] J. Yang, W. Zhang, J. Liu, J. Wu, and J. Yang, "Generating De-identification facial images based on the attention models and adversarial examples," *Alexandria Engineering Journal*, vol. 61, no. 11, pp. 8417–8429, 2022.

[20] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, 2018.

[21] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 24–32, 2018.

[22] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for Healthcare 4.0 environment: opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.

[23] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[24] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Networks*, vol. 22, no. 2, pp. 491–502, 2016.

[25] A. Armando and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *Computer Aided Verification*, K. Etessami and S. K. Rajamani, Eds., vol. 3576pp. 281–285, 2005.

[26] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *International Journal of Communication Systems*, vol. 32, no. 6, p. e3900, Apr, 2019.

[27] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: temporal credential-based anonymous lightweight authentication scheme for internet of Drones environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[28] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, Berlin, Germany, 2003.

[29] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: the serpentine course of a paradigm shift," *Journal of Number Theory*, vol. 131, no. 5, pp. 781–814, 2011.

[30] M. Burrows and M. Abadi, "A logic of authentication," *Proceedings of the Royal Society A: Mathematical, Physical Science*, vol. 426, pp. 233–271, 1989.

[31] E. Bresson, O. Chevassut, and D. Pointcheval, "Security proofs for an efficient password-based key exchange," in *Proceedings of the 10th ACM conference on Computer and communications security*, Washington D.C. USA, October 2003.

[32] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography*, Les Diablerets, Switzerland, January 2005.

[33] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2017.

[34] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things

environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[35] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[36] H. Nicanfar and V. C. M. Leung, "Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 253–264, 2013.

[37] X. Li, J. Niu, S. Kumari, J. Liao, and W. Liang, "An enhancement of a smart card authentication scheme for multi-server architecture," *Wireless Personal Communications*, vol. 80, no. 1, pp. 175–192, 2015.

[38] B. Zhao, S. Zeng, H. Feng et al., "Lightweight mutual authentication strategy for internet of electric things," *Sustainable Energy Technologies and Assessments*, vol. 45, Article ID 101130, 2021.

[39] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: testing the limits of elliptic curve cryptography in sensor networks," in *Wireless Sensor Networks*, R. Verdone, Ed., vol. 4913pp. 305–320, 2008, http://link.springer.com/10.1007/978-3-540-77690-1_19.

Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 1066547, 10 pages
https://doi.org/10.1155/2023/1066547

Research Article

An IoMT-Based Approach for Real-Time Monitoring Using Wearable Neuro-Sensors

Mohammed Wasim Bhatt and Sparsh Sharma

Department of Computer Science and Engineering, National Institute of Technology, Srinagar, India

Correspondence should be addressed to Mohammed Wasim Bhatt; wasim_2021phacse004@nitsri.net and Sparsh Sharma; sparsh.sharma@nitsri.net

Received 21 July 2022; Revised 15 August 2022; Accepted 28 January 2023; Published 13 February 2023

Academic Editor: Irshad Azeem

The Internet of Things (IoT) has demonstrated over the past few decades to be a powerful tool for connecting various medical equipment with in-built sensors and healthcare professionals to deliver superior health services that also reach remote areas. In addition to reducing healthcare costs, increasing access to clinical services, and enhancing operational effectiveness in the healthcare industry, it has also enhanced patient health safety. Recent research has focused on using EEG to assist and comprehend brain changes in rehabilitation facilities. These technologies can spot fluctuations in EEG constraints during treatment, which could result in more effective therapy and better functional outcomes. As a result, we have tried to use an IoT-based system for real-time monitoring of the constraints. Another unknown patient who is suffering from acute ischemic stroke may experience stroke-in-evolution or an early worsening of neurological symptoms, which is frequently associated with poor clinical outcomes. Because of this, managing an acute stroke requires early detection of these indications. The present investigation work will act as a standard reference for academic researchers, medical professionals, and everyone else involved in the use of IoMT. This study aims to anticipate strokes sooner and prevent their consequences by early intervention using an Internet of Things (IoT)-based system. Also, this study proposes usage of wearable equipment that can monitor and analyze brain signals for improved treatment and the prevention of stroke-related complications.

1. Introduction

As crucial as ongoing technical innovations are for improving healthcare and lowering costs, they also provide a hurdle for integrating new technologies into clinical treatment [1–3]. In order to address the drawbacks of conventional healthcare and satisfy the growing demand for high-quality healthcare, a significant amount of research is presently concentrated on intelligent healthcare. Traditional healthcare, wearable technology, biosensors, and intelligent quick action services are all entities that can be included in the notion of smart healthcare. For the majority of the people, medicinal plants are frequently the only readily available alternative to conventional medicines, which continue to be an essential part of our comprehensive health system. Indigenous people have demonstrated historical continuity in material use and have a thorough understanding of the intricate biological system that surrounds their environment. Because of their ability to deliver continuously, today's research information in a variety of healthcare-related applications through dynamic, noninvasive measurements of chemical markers in biofluids, wearable biosensors are generating a lot of interest. Early research in this field concentrated on using physical sensors to track movement and vital signs. Experts are now focusing on overcoming significant obstacles in healthcare applications, moving away from monitoring the physical activity through wearable devices. IoMT, a group of healthcare apps and equipment that links to medical information technological systems through the network, serves as the foundation of innovative healthcare [4, 5]. One example of intelligent healthcare is the automatic identification of epileptic episodes.

Recurrent spontaneous seizures characterize a neurological condition known as epilepsy. A seizure is an abrupt disruption of brain activity that lasts for just a short time and may be accompanied by convulsions and loss of consciousness [6]. The quality of life for people with epilepsy suffers significantly as a result. Sudden unexplained death (SUDEP) is more common among people with epilepsy than in the general population [7, 8], which minimizes the severity of this disease. Seizures can be controlled using antiepileptic medicines (AEDs), although 30% of epilepsy patients are resistant to AEDs [9–11]. Only a very tiny percentage of individuals with refractory epilepsy benefit from surgery. Implantable technology in the brain has great potential for seizure management. Predicting and detecting seizures is crucial because early identification and warning can lead to prompt treatment [12–14].

Technology for mass consumer electronic (CE) goods is presented in this article as a type of neurosensory wearables for intelligent biomedical systems. A medical-grade wristwatch for an illness related to neurological disorder warns caretakers when a patient is experiencing an epileptic seizure is one example of a wearable CE device [15, 16]. A predicted 57 billion USD would be spent on the Internet of Medical Things (IoMT)-driven smart healthcare sector [17]. The CE research that has already been carried out is effectively advanced by this article. It should be mentioned that this article presents the CE record of the technique and sample with validation, using accessible healthcare information and working with medical schools. Understanding the brain function and dysfunction requires knowledge of the brain's many physiological states, which the EEG contains in abundance. Visual inspection can identify seizures, but it takes a lot of time and effort [18]. The two stages of interictal (between seizures) and ictal (seizure) are the main areas of attention in epilepsy. The accuracy of classification can be significantly influenced by the specific information captured by extracted features [19, 20]. This information is vital for differentiating EEG dynamics. Feature extraction is therefore essential for categorization. The following are a few instances: Chesti Altaf Hussain's intelligent IoT and the Android healthcare monitoring solution. The above-mentioned projects are the IoT-based systems [21] that monitor people's heart rates, body temperatures, and heart attacks [22] with the aim to monitor and improve the protective quality provided to population in backward areas and provide information for good health maintenance choices in severely adverse conditions.

In this study, we intend to contribute significantly in the field of neuroscience research.

The architecture and fundamental components of the Internet of Things system are depicted in Figure 1. The topologies of the remote health monitoring system in the medical industry consist of three layers: the layer for the gathering of vitals data, the layer for transmission, and the layer for analysis. The collection layer is constructed out of body area network (BAN) sensors. The data collected by sensors are transmitted to a gateway node by the BAN. The data are saved by the transmission layer, and threshold levels are used to analyze it and report any irregularities. There is also the possibility of the data being processed and stored in the cloud. An intelligent system is one that can detect irregularities and predict a patient's health using techniques such as machine learning and data mining. In the final step, the data analysis is uploaded to a server located in the cloud. A web-based interface allows medical practitioners to check diagnostics and take the right action depending on their findings. The software sector is currently evolving toward artificial intelligence. Every industry now relies on machine learning to give machines intelligence. Machine learning, to put it simply, is a group of algorithms that analyze data, gain knowledge from it, and then use what they have learned to make wise decisions. Traditional machine learning algorithms have the drawback of remaining machine-like despite their apparent complexity. They are only able to perform what they are created for; nothing more, nothing less; they require a lot of domain expertise and human intervention.

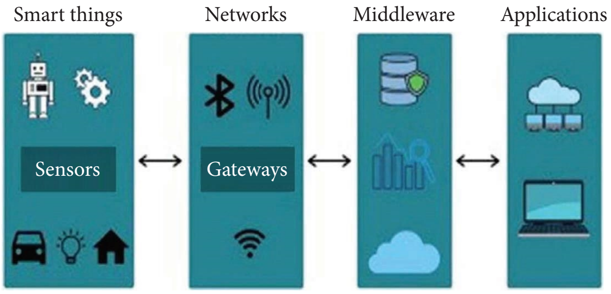


Figure 1: IoT architecture [23].

Figure 2 depicts the system that enables communication across systems, applications, and devices that are all connected to the same network. With the help of this system, patients and their doctors will have an easier time keeping track of and recording extremely important medical information pertaining to patients. A variety of various goods now include a variety of different types of gadgets, such as those for tracking positive metrics, wearable health bands, exercise shoes, watches that are based on RFID technology, and high-end video cameras. Applications that are created specifically for mobile devices, such as smartphones, make it much simpler to keep a case history, complete with access to emergency services and regular warnings. The enormous quantities of data that are produced by these interconnected Internet of Things devices have to be successfully managed by the service providers, which may prove to be an incredibly challenging task. The process of storing and assessing significant volumes of data that is referred to as Internet of Things analytics (particle) is implemented. This is carried out so that the problem can be solved. The unprocessed data are converted into information that is not only helpful but also restoratively significant through the application of methods such as information extraction and information analytics. The following are the prime contributions of the article:

(i) The purpose, restrictions, and potential future application of research are highlighted in this article's overview of earlier studies that have used IoT in healthcare.

(ii) This research also suggests strategies to monitor patients in real-time settings.

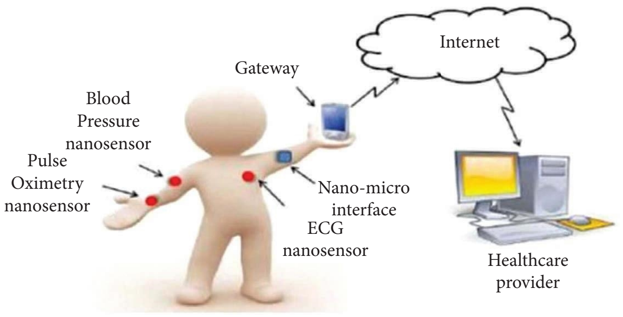


Figure 2: IoT building blocks [24].

(iii) This research focuses on using IOMT to make it easier to continuously monitor potential patients' health.

(iv) By offering insights into or solutions to several investigations, the research offers an investigative strategy.

(v) Current investigative article outlines a number of obstacles faced by IoMT.

(vi) The present investigation work will act as a standard reference for academic researchers, medical professionals, and everyone else involved in the use of IoMT.

(vii) To anticipate strokes sooner and prevent their consequences by early intervention, we have tried to establish real-time monitoring of a few metrics using an Internet of Things (IoT)-based system.

(viii) The current study aims to propose wearable equipment that can monitor and analyze brain signals for improved treatment and the prevention of stroke-related complications.

The rest of this article is structured as follows: Most recent seizure detection research is described in Section 2 and the proposed research methodology used to select articles is summarized in Section 3. An architectural review of the suggested proposal is provided in Section 4. The discussion of article is covered in Section 5. Conclusions and recommendations for the further study are presented in Section 6.

2. Literature Review

Rani et al. proposed a unique time-frequency spectrum estimation approach for multichannel data [25]. Furthermore, it is applicable to the epileptic type of electroencephalography (EEG). Smooth localized complex exponential (SLEX) functions, which are time-frequency localized variants of the Fourier functions, are used to construct the approach. As a result, they are particularly well adapted to studying nonstationary signals whose spectral properties shift over time. Because the input signals are generated using a projection operator rather than a window or taper, the SLEX functions are orthogonal and concurrently confined in time and frequency [26].

The domain of picture enhancement in digital image processing is one of the most simple and pleasurable to work in. The goal is to highlight specific details in an image or certain attractive traits (Pandey et al. [27]). The quality of the deformed image may be improved by adjusting the luminance of the bone or the brain tissue in the input image [28]. This enhancement method uses a dualistic subimage histogram equalization methodology. A segmentation approach based on directional homogeneity and using an improved metric has been created. The two seed templates must be uniformly orientated in opposed directions for this procedure to operate. There are just a few directions in which one can look for pixels. The production of brain image pixels is swift and accurate since just eight directions are considered. A technique that requires less computer efficiency is used to compare the picture sections to the templates [29]. Anderson are some of the authors contributing to this study. A wearable helmet for humans could be a crucial tool for monitoring employees' health in the mining industry. However, identifying human emotions in hostile environments has received little research [30]. Another benefit of using this technique would be that the hybrid model for anxiety levels has an appropriate follow-up role in the unpleasant psychological shift [31]. This method may be used to measure how much anxiety a person is experiencing. This method can therefore improve operational safety and prevent incorrect miner operating. It is now possible to collect behavioural, physiological, and social activity indicators invisibly, thanks to the explosive expansion of integrated smart sensors that are found in mobile devices and wearable technology [32]. Self-help applications, electronic cognitive behavioural therapy [33], relaxation aids, video-based instruction [34], virtual reality [35], brain-computer interface (BCI) technologies, and other methods might all be used to offer many of these treatments electronically [36, 37]. The key elements of a perfect sensor are selectivity, linearity, sensitivity, precision, repetition and reproducibility, calibrating, drift, and fast response [38]. Machine learning approaches may help to create a positive feedback loop that makes it possible to continuously improve the therapeutic interventions for a given patient [39]. Any digital item, including wearables and hardware, with a variety of applications that spans many facets of society can be an IoT device [40]. The healthcare sector is quickly adopting IoT-based solutions. Additionally, an IoMT estimate for 2020 has been prepared. By 2022, it is anticipated that the market for connected devices used for patient care, monitoring, and diagnosis would increase from $14.9 billion to $52.2 billion [41]. IoMT security has become extremely difficult since new security issues are emerging while old security issues have intensified along with its rapid growth and diverse nature. To ensure integrity, validity, and data privacy, data must be stored and transferred without any unwanted access [42].

3. Publications Related to the Study

Reviewable research publications that stressed on the integration of Internet of Things in healthcare have been included. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria were used to identify the publications for the investigation.

Using the flowchart given in Figure 3 for PRISMA, an extensive choice of research articles is made at various phases.

(i) An inclusive examination of research articles on freely available search engines such as Google Scholar, PubMed, Web of Science, Science Direct, and Scopus was carried out during June, 2022. Also, some articles were short listed using hand searches.

(ii) The keywords used for the selection of articles at "IoMT," "brain signals," "stroke prediction," and "wearable sensors".

Similar articles are eliminated in the first step, leaving only research works published after 2010 for the subsequent screening stage. The choice to include or omit the research articles has been made after research publications have been rejected at a later stage based on title, abstract, and full-text readings at the eligibility stage. The last and inclusion step was when selected research articles were examined for the current study taking into account all the inclusion criteria.

Through the real-time modification of patient behavior and health conditions, the IoMT bridges the gap between the digital and physical worlds to improve patient health. IoMT is a group of interconnected devices that provide online health services. IoMT is a connected health system infrastructure that consists of medical tools, software programs, and services, and it strives to give patients and those who are at risk of developing major health issues better individualized or tailored care. More precisely, linking devices and sensors enables the healthcare industry to boost workflow management and clinical operations efficiency while also enabling remote patient health monitoring. Both patients and clinicians are greatly impacted by the connectivity of medically important devices. One of the key benefits of IoMT-based remote health monitoring is the ability for patients to perform routine tasks while their health is being continuously monitored. Another important benefit is the reduction in hospital costs. Traditional remote monitoring systems are uncomfortable for patients due to the size of the modules linked to the body and the frequent charging or replacement of batteries. Deep learning algorithms do not perform too well with little data. This is because deep learning algorithms require a lot of data to fully comprehend it. With each idea established in connection to simple ideas and much more complex depictions computed in terms of less abstraction ones, deep learning, a type of machine learning, learns to depict the world as a layered network of ideas. Many people believe that deep neural networks are the be all and end all and that they should completely replace existing methods. Before abandoning conventional algorithms, it is critical to comprehend how to combine the two to get forecasts that are more accurate. The IoT revolution tackles the aforementioned issues by creating compact, low-power sensor hardware and streamlining communication methods. The sensors and electronic circuits in the portable patient monitoring device can collect vital signs. Figure 4 depicts a schematic illustration of IoMT in a live setting. Using an interactive interface, the doctor may see the patient's condition. The remote health monitoring system is made up of portable monitoring devices for patients and a real-time monitoring system at the hospital that helps to make decisions.

The most important sort of monitoring is cardiac monitoring since it can reveal many diseases that are naturally disguised, such as arrhythmia. In order to further research and give patients new treatment options, IoMT-based devices are being developed to monitor the behavior of mental patients. A textile-based autonomic nervous system is one of the crucial parameter collection tools used for remote monitoring of neurological and brain disorders. Additionally, it offers diabetes sufferers remote monitoring tools. A critical area of IoMT is the identification of falls in elderly people who are being monitored in real-time. A variety of sensors, including gyroscope sensors, accelerometers, and respiration rate sensors, are included in the data collection system. Several systems, especially for elderly patients, use different arrangements of sensor nodes to find out when a patient falls. In some hospitals, real-time statistical data are generated, shared on a public ledger, and examined by the healthcare professional. The doctor keeps an eye on the patient using some wearable tracking gadgets. Wearable technology detects changes in the patient's body and sends the doctor real-time data. The patient is then given advice by the doctor based on their health. The patient's caregivers can also see the patient history. Every node in the patient network can see the reports and therapy for the patient that are shared on the public ledger. Table 1 presents a list of efficient IOT-based sensors for the brain and fitness.

4. Discussion

By 2025, the market for IoT-based smart healthcare is expected to be worth 350 billion US dollars. Smart cabinets and medicines incorporated into the IoT framework for the healthcare industry are getting much attention. Several CE systems have been presented for older health care [43, 44]. Data transfer from the corresponding sensors for electrocardiograms (ECG), electroencephalograms (EEG), and electromyograms (EMG) has been suggested [45]. For ongoing geriatric monitoring, a wireless sensor network (WSN) is provided. CE solutions for automated seizure detection are nonetheless required for the IoT framework in order to improve the state-of-the-art in intelligent medical healthcare. The suggested approach improves CE by including epileptic seizure diagnoses and remote analysis of health.

Epileptic seizure detection has been carried out using several different techniques. The approximate entropy (ApEn) value considerably decreases during seizure activity, according to research on a seizure detection algorithm based

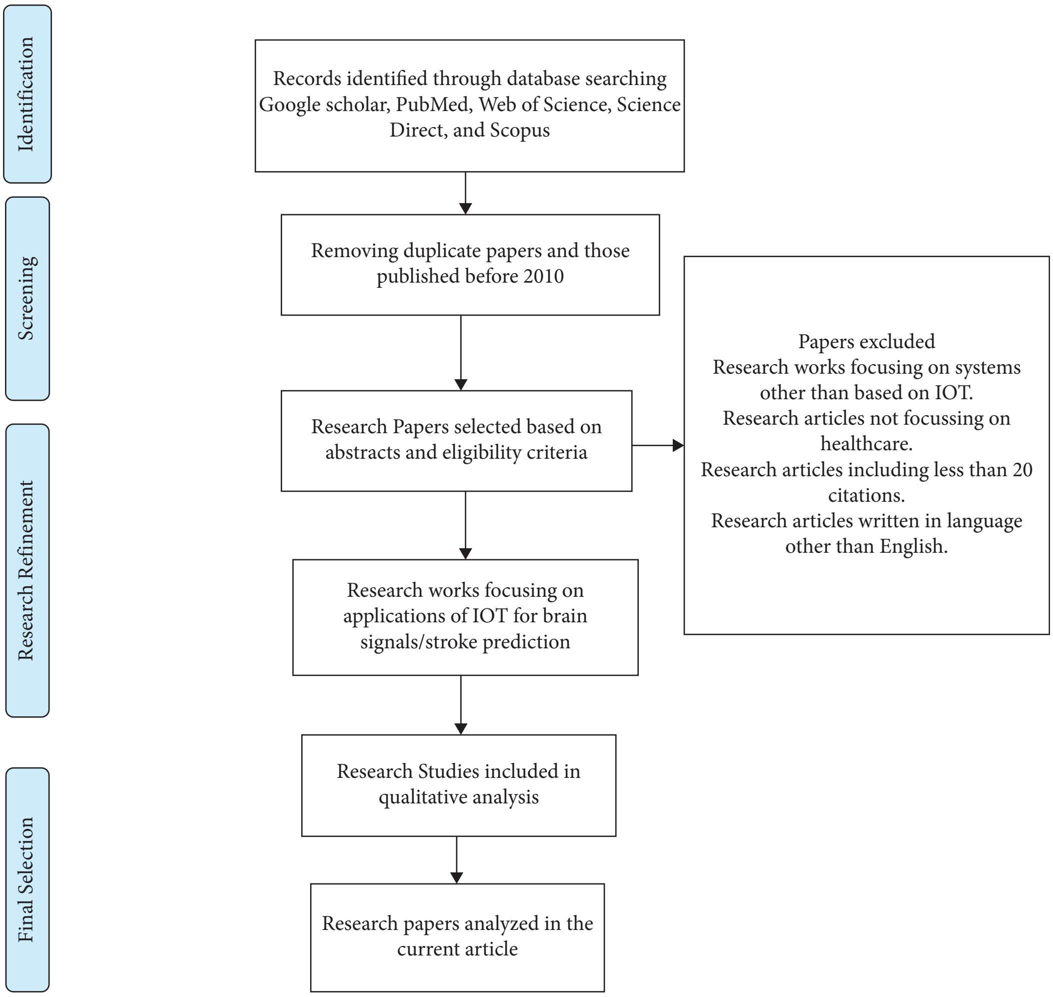

Identification
Screening
Research Refinement
Final Selection
Records identified through database searching Google scholar, PubMed, Web of Science, Science Direct, and Scopus
Removing duplicate papers and those published before 2010
Research Papers selected based on abstracts and eligibility criteria
Research works focusing on applications of IOT for brain signals/stroke prediction
Research Studies included in qualitative analysis
Research papers analyzed in the current article
Papers excluded
Research works focusing on systems other than based on IOT.
Research articles not focussing on healthcare.
Research articles including less than 20 citations.
Research articles written in language other than English.

Figure 3: PRISMA search strategy.

on ApEn [46]. According to a correlation dimension (CD)-based technique, the epileptogenic zone has low CD values. For identifying seizures, classifiers based on artificial neural networks (ANN) have been suggested [47, 48], with better classification accuracy. Seizure detection using a multilayer perception neural network (MLPNN) [49] has improved detection performance. For differentiating between seizure and nonseizure patterns, ANN and wavelet transform-based feature extraction [49] was applied. The smoothed-pseudo-Wigner–Ville distribution is analyzed for feature extraction in the short-term Fourier transform (STFT)-based technique [50]. A multilayer perception network (MLP) and a radial basis function (RBF) network have both been used to classify seizures [51]. According to permutation entropy-based categorization, a considerable decrease in permutation entropy is seen during seizures [52]. Seizure detection has been improved with an SVM-based technique, which was proposed in references [53, 54]. Seizure detection accuracy was increased and power consumption was decreased via a signal rejection algorithm-based seizure detector [55, 56].

Figure 5 provides an illustration of a fundamental overview of the system. Disorders associated with stress and anxiety are becoming increasingly prevalent in today's society. Because of this, improper management of stress can result in stress disorders, emotional suffering, and physical diseases. The authors created an IoMT-powered edge device with deep learning stress management algorithms. Physiological data are used to detect stress at the edge and transferred to the cloud for deep learning analysis. The scientists created a wristband with sensors (contact-temperature, humidity, and accelerometer) to detect stress patterns in users. Using a deep neural network (DNN) algorithm, Stress-Lysis sensor data generate discrete stress values (low, normal, and high). The authors applied their algorithm to diverse datasets and tested its efficiency using real-time metrics to validate the proposed system's accuracy. Their investigation shows that their proposed approach is 98.3%–99.7% accurate in identifying user stress. The classification of food items is performed by a machine learning model called Single Shot MultiBox MobileNet. To calculate calories, researchers first compare the data they acquire to a nutrition database. User stress is detected by the extraction and analysis of many features. Meal details, such as kind, quantity, timing, and user sex, are all included. Table 2 illustrates the findings of the monitoring system for stress and anxiety in the current state-of-art techniques.

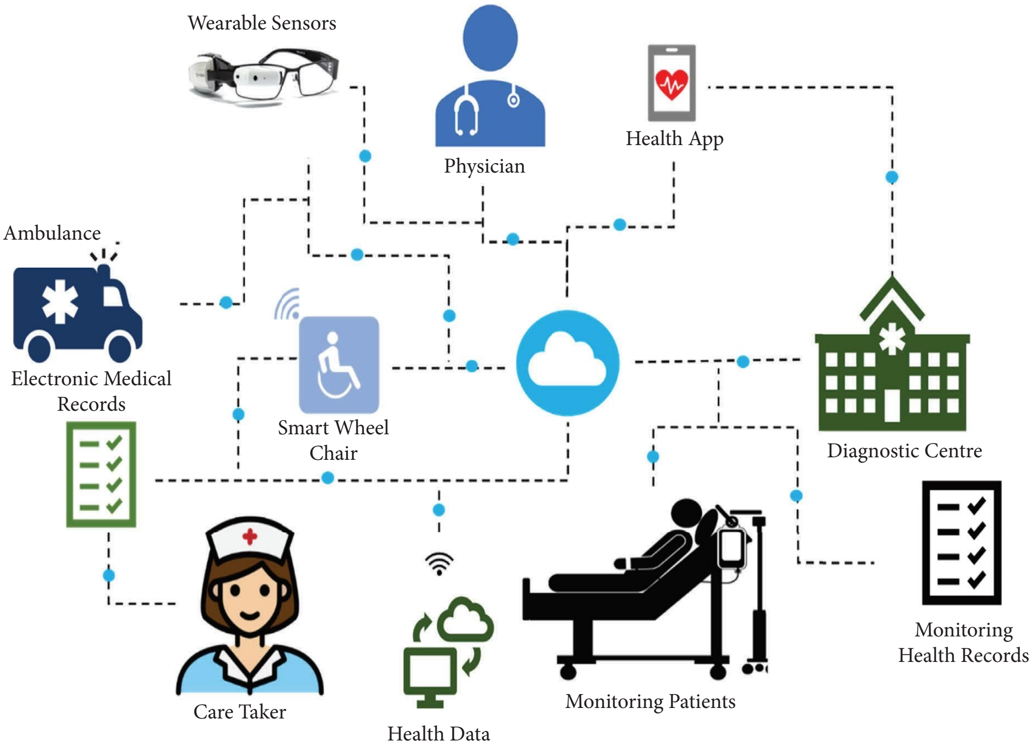


Figure 4: IoMT application in real time.

Reference [58] suggests developing an Internet of Things (IoT)-based low-cost anxiety disorder monitor. This monitor would deduce emotional aspects from physiological indicators in a semi-immersive environment. The IoT node collects data on the user's heart rate as well as their level of physical activity. This information is then transmitted to a Raspberry Pi 3, where it is preprocessed before being sent to the IoT cloud. The findings of this system's validation revealed that it has an accuracy rate of 90% when it comes to recognising anxiety disorders. The proposed categorization system is elected to take this technique [59] in order to improve its overall accuracy. This ensemble strategy for detecting the emotions of the user improves the classification accuracy of emotion-aware IoMT-based architectures by 7–9%, according to the validation results of the system that was proposed. A unique IoMT-based strategy for managing chronic stress for females and the older adults has been presented [60].

The primary concept behind ML is that you create a dataset, give it to ML algorithms to learn from, and afterwards the ML algorithms use the data analysis to produce predictions or suggestions. One effect is that machines may learn to be biased or act against a few people's interests based on the data input. Results from a machine algorithm that include bias may not be in accordance with societal moral norms. Long offline/batch training is necessary to avoid real-time, interactive or progressive learning, Poor integration, reusability, and transferability of learning. Systems are transparent, which makes them difficult to troubleshoot. As an example of a machine learning (ML)-based smart gadget that can be implemented in smart cities and enterprises, the authors recommend iMirror [61]. Because this tool lowers stress, it helps people with stress-related chronic conditions. Mirror-mounted cameras can be used for facial recognition, stress research, and app updates. When a user takes a picture, the device automatically identifies them and scans the image to pull out information for an ML model that can categorise the user's stress level depending on the image. We tallied up the number of cases with red eyes, puffy eyes, dilated pupils, frown lines, and perspiration on the face. An ML model (a lightweight and optimised version of SSD Mobilenet) is fed to these features in order to characterize the stress level and update the mobile app. The technology is useful since it customises therapies for individuals. The model had a 97% accuracy rate and an 81.2% precision, as determined by experiments. In order to determine if a person has a stress problem, it is important to keep track of what they consume and how often they eat. Automatically tracking a user's dietary intake and then converting that into an estimate of their stress level [62] makes use of the camera on a smartphone or a single board computer equipped with a camera. Edge computing devices can use the iLog deep learning model to identify and measure the quantity of food items on a plate. Using plate data, iLog can determine the user's stress level [63–65]. The cutting-edge method developed by the researchers instantly tallies calories, recognizes food, and establishes a connection between diet and anxiety. This method uses IoMT to send images captured by iLog glasses to a device at the network's edge. Images are broken up by the edge computing device, and the TensorFlow Object Detection API is used to identify objects in the images [66, 67].

Table 1: IoT-supported brain and fitness sensing devices.

Names	References	Reliability	Availability	IoT-supported	Cost	Data usage
Thync	https://www.thync.com/	No validation	True	True	Costly	Low
Muse	https://www.muse.mu/	No validation	True	True	Average expense	Average
NeuroSky	https://neurosky.com/	No validation	True	True	Cheap	Average
YBrain	https://www.ybrain.com/	No validation	True	True	Average expense	Low
Halo	https://www.haloneuro.com/	No validation	True	True	Average expense	Low
Sensoria health	https://www.sensoriahealth.com/	No validation	True	True	Cheap	Average
Lumo	https://www.lumobodytech.com/	No validation	True	True	Costly	Average
OMsignal	https://www.omsignal.com/	No validation	True	True	Costly	Average
Motiv	https://www.mymotiv.com/	No validation	True	True	Cheap	Average
Athos works	https://www.liveathos.com/	No validation	True	True	Cheap	Low
Atlas wearables	https://www.atlaswearables.com/	No validation	True	True	Cheap	Low
Moov	https://www.welcome.moov.cc/	No validation	True	True	Costly	Low
Withings	https://www.withings.com/	No validation	True	True	Very costly	Max
Misfit	https://www.misfit.com/	No validation	True	True	Cheap	Max
Biostrap	https://www.biostrap.com/	No validation	True	True	Cheap	Max
Zanthion	https://www.zanthion.com/	No validation	True	True	Average expense	Max
Verily	https://www.verily.com/	No validation	True	True	Average expense	Average
Triggerish	https://www.sensimed.ch/%20sensimed-triggerfish/	No validation	True	True	Cheap	Average

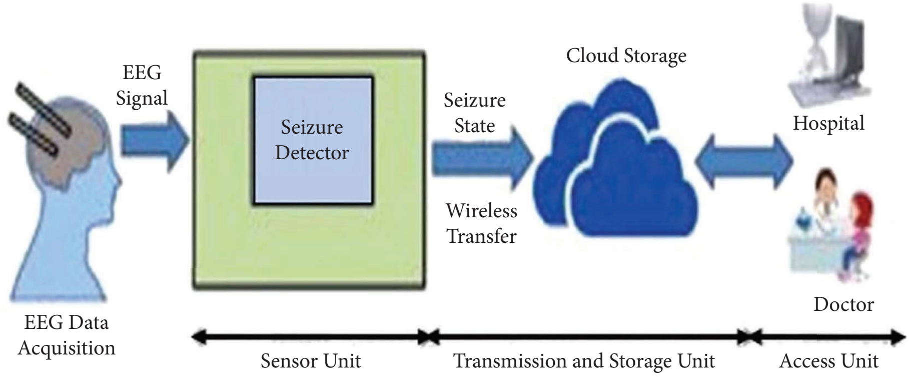


Figure 5: Architecture of seizure [57].

Table 2: Results of a monitoring system for stress and anxiety.

Ref no	Models proposed	Results obtained
[58]	IoT-based low-cost anxiety disorder monitor	Accuracy 90%
[59]	EEG-powered smart emotion-aware IoMT-based framework for health monitoring	Accuracy increased by 7–9%
[60]	IoMT-based novel system has been proposed for chronic stress management in women and the elderly	Accuracy ranges from 98.3% to 99.7%
[61]	ML-based smart device that detects stress levels in users to aid the IoMT framework of smart cities and offices	Accuracy 97% and precision 81.2%
[62]	Stress monitoring	Accuracy 98% andprecision 85.8%

5. Conclusion

A few physical items have also been equipped with IoT devices (sensors, actuators, etc.), enabling real-time monitoring and data transmission across different communication protocols, including Bluetooth as well as Wi-Fi. A patient's electroencephalogram (EEG), heart rate, and electrocardiogram (ECG) are just a few examples of the critical physiological data that these sensors are used to collect in the healthcare industry. These sensors can be worn on the body or embedded in clothing. In addition, environmental information such as temperature, humidity, date, and time can also be analyzed. This exemplifies the potential and utility of IoT, especially related to smart health-based industry. Everyone in society is currently so focused on getting by that they are neglecting their health. With the development of intelligent sensors, it is now possible to continuously monitor a person's behavior, record data, and predict the onset of a heart attack even prior to the patient feels its effects. Therefore, it is crucial to choose and apply the appropriate sensors. Another decentralized method called "block-chain storage" is developed to produce independent yet distinct groups of data called "blocks." As a result, a network governed by patients as opposed to a third party is created. Although still in its infancy, the use of edge cloud and blockchain in the healthcare industry is developing as a new topic for research.

Data Availability

The data used in this article will be made available upon request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything you wanted to know about Smart Healthcare," *IEEE Con- sum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, Jan. 2018.

[2] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 60–70, July 2016.

[3] H. Yan, H. Huo, Y. Xu, and M. Gidlund, "Wireless sensor network based e-Health system - implementation and experimental results," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2288–2295, Nov, 2010.

[4] "Internet of health things: privacy and security issues in an interconnected world," 2017, https://www.icemiller.com/ice-on-fire-insights/publications/the-internet-of-health-things-privacy-and-security/.

[5] "IoMT (internet of medical things) or healthcare IoT," 2017, https://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things.

[6] ILAE Commission, "The epidemiology of the epilepsies: future directions," *ILAE, Tech. Rep.*, vol. 5, 1997, https://www.ncbi.nlm.nih.gov/pubmed/9184609.

[7] L. A. Jones and R. H. Thomas, "Sudden death in epilepsy: insights from the last 25 years," *Seizure*, vol. 44, no. 3, pp. 232–236, Jan. 2017.

[8] P. Kwan and M. J. Brodie, "Early identification of refractory epilepsy," *New England Journal of Medicine*, vol. 342, no. 5, pp. 314–319, Feb. 2000.

[9] F. Mormann, R. G. Andrzejak, C. E. Elger, and K. Lehnertz, “Seizure prediction: the long and winding road,” *Brain*, vol. 130, no. 2, pp. 314–333, Feb. 2007.

[10] I. Osorio, H. P. Zaveri, M. G. Frei, and S. Arthurs, *Epilepsy: The Intersection of Neurosciences, Biology, Mathematics, Engineering, and Physics*, CRC Press, Boca Raton, Fl, USA, 2011.

[11] R. S. Fisher, “Therapeutic devices for epilepsy,” *Annals of Neurology*, vol. 71, no. 2, pp. 157–168, Feb. 2012.

[12] B. J. Gluckman and C. A. Schevon, “Seizure prediction 6: from mech- anisms to engineered interventions for epilepsy,” *Journal of Clinical Neurophysiology*, vol. 32, no. 3, pp. 181–187, Jun 2015.

[13] N. Verma, A. Shoeb, J. Bohorquez, J. Dawson, J. Guttag, and A. P. Chandrakasan, “A micro-power EEG acquisition SoC with integrated feature extraction processor for a chronic seizure detection system,” *IEEE Journal of Solid-State Circuits*, vol. 45, no. 4, pp. 804–816, Apr. 2010.

[14] M. T. Salam, M. Sawan, and D. K. Nguyen, “A novel low-power- implantable epileptic seizure-onset detector,” *IEEE Trans. Biomed. Cir- cuits Syst.*, vol. 5, no. 6, pp. 568–578, 2011.

[15] E. Dolgin, “This seizure-detecting smartwatch could save your life,” spectrum.ieee.org,” 2018, https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/this-seizuredetecting-smartwatch-could-save-your-life.

[16] “Smart Healthcare Products Market Is Expected to Get US$ 57 Billion by 2023,” marketwatch.Com,” 2018, https://www.marketwatch.com/press-release/smart-healthcare-%20products-market-is-expected-to-get-us-57-billion-by-2023-2018-08-28.

[17] A. Shoeb, H. Edwards, J. Connolly, B. Bourgeois, S. Ted Treves, and J. Guttag, “Patient-specific seizure onset detection,” *Epilepsy and Behavior*, vol. 5, no. 4, pp. 483–498, 2004.

[18] A. Subasi and M. Ismail Gursoy, “EEG signal classification using PCA, ICA, LDA and support vector machines,” *Expert Systems with Applications*, vol. 37, no. 12, pp. 8659–8666, Dec, 2010.

[19] H. Ocak, “Automatic detection of epileptic seizures in EEG using discrete wavelet transform and approximate entropy,” *Expert Systems with Applications*, vol. 36, no. 2, pp. 2027–2036, Mar, 2009.

[20] C. V. Granger, L. S. Dewis, N. C. Peters, C. C. Sherwood, and J. E. Barrett, “Stroke rehabilitation: analysis of repeated Barthel index measures,” *Archives of Physical Medicine and Rehabilitation*, vol. 60, no. 1, pp. 14–17, 1979.

[21] F. I. Mahoney and D. W. Barthel, “Functional evaluation: the Barthel index. Md,” *Statistics in Medicine J*, vol. 14, pp. 61–65, 1965.

[22] S. D. Cranstoun, H. C. Ombao, R. Von Sachs, W. Wensheng Guo, and B. Litt, “Time-frequency spectral estimation of multichannel EEG using the auto-SLEX method,” *IEEE Transactions on Biomedical Engineering*, vol. 49, no. 9, pp. 988–996, 2002.

[23] Z. Ashfaq, A. Rafay, R. Mumtaz et al., “A review of enabling technologies for internet of medical things (IOMT) ecosystem,” *Ain Shams Engineering Journal*, vol. 13, no. 4, Article ID 101660, 2022.

[24] S. K. Polu and S. K. Polu, “IoMT based smart health care monitoring system,” *International Journal for Innovative Research in Science & Technology*, vol. 5, no. 11, pp. 58–64, 2019.

[25] P. Rani, N. Hussain, R. A. H. Khan, Y. Sharma, and P. K. Shukla, “Vehicular intelligence system: time-based vehicle next location prediction in software-defined internet of vehicles (SDN-IOV) for the smart cities,” in *Intelligence of Bings: AI-IoT Based Critical-Applications and Innovations*, F. Al-Turjman, A. Nayyar, A. Devi, and P. K. Shukla, Eds., Springer, Berlin, Germany, 2021.

[26] E. C. Hames, B. Murphy, R. Rajmohan et al., “Visual, auditory, and cross modal sensory processing in adults with autism: an EEG power and BOLD fMRI investigation,” *Frontiers in Human Neuroscience*, vol. 10, p. 167, 2016.

[27] D. Pandey, U. Rawat, N. K. Rathore, K. Pandey, and P. K. Shukla, “Distributed biomedical scheme for controlled recovery of medical encrypted images,” *IRBM*, vol. 43, 2020.

[28] H. Kaushik, D. Singh, M. Kaur, H. Alshazly, A. Zaguia, and H. Hamam, “Diabetic retinopathy diagnosis from fundus images using stacked generalization of deep models,” *IEEE Access*, vol. 9, pp. 108276–108292, 2021.

[29] M. Arnold, X. H. R. Milner, H. Witte, R. Bauer, and C. Braun, “Adaptive AR modeling of nonstationary time series by means of Kalman filtering,” *IEEE Transactions on Biomedical Engineering*, vol. 45, no. 5, pp. 553–562, 1998.

[30] T. W. Anderson, *Be Statistical Analysis of Time Series*, Wiley, New York, NY, USA, 1971.

[31] P. A. Anninos and S. Zenone, “A neural net model for the Alpha – rhythm,” *Biological Cybernetics*, vol. 36, no. 4, pp. 187–191, 1980.

[32] S. Abdullah and T. Choudhury, “Sensing technologies for monitoring serious mental illnesses,” *IEEE MultiMedia*, vol. 25, no. 1, pp. 61–75, 2018.

[33] L. Hillert, B. Kolmodin Hedman, B. F. Dölling, and B. B. Arnetz, “Cognitive behavioural therapy for patients with electric sensitivity–A multidisciplinary approach in a controlled study,” *Psychotherapy and Psychosomatics*, vol. 67, no. 6, pp. 302–310, 1998.

[34] C. Yuh-Tyng, “The effect of thematic video-based instruction on learning and motivation in e-learning,” *International Journal of the Physical Sciences*, vol. 7, no. 6, pp. 957–965, 2012.

[35] D. Peeters, “Virtual reality: a game-changing method for the language sciences,” *Psychonomic Bulletin & Review*, vol. 26, no. 3, pp. 894–900, 2019.

[36] T. Fleming, L. Bavin, M. Lucassen, K. Stasiak, S. Hopkins, and S. Merry, “Beyond the trial: systematic review ofreal-world uptake and engagement with digital self-help interventions for depression, low mood, or anxiety,” *Journal of Medical Internet Research*, vol. 20, no. 6, p. e199, 2018.

[37] E. G. Lattie, E. C. Adkins, N. Winquist, C. Stiles-Shields, Q. E. Wafford, and A. K. Graham, “Digital mental health-interventions for depression, anxiety, and enhancement of psychological well-being among college students:Systematic review,” *Journal of Medical Internet Research*, vol. 21, no. 7, Article ID e12869, 2019.

[38] C. Rosenzweig, D. Karoly, M. Vicarelli et al., “Attributing physical and biological impacts to anthropogenic climate change,” *Nature*, vol. 453, no. 7193, pp. 353–357, 2008.

[39] H. O. Alanazi, A. H. Abdullah, and K. N. Qureshi, “A critical review for developing accurate and dynamicpredictive models using machine learning methods in medicine and health care,” *Journal of Medical Systems*, vol. 41, no. 4, p. 69, 2017 [CrossRef].

[40] L. Atzori, “The internet of things: a survey,” *Computer Networks*, vol. 54, 2010.

[41] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, “Prospect of internet of medical things: a review on security requirements and solutions,” *In Sensors*, vol. 22, no. 15, p. 5517, 2022.

[42] W. Sun, Z. Cai, Y. Li, F. Lui, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018, Article ID 5978636, 9 pages, 2018.

[43] P. C. Petrantonakis and L. J. Hadjileontiadis, "Emotion recognition from EEG using higher order crossings," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 2, pp. 186–197, 2010.

[44] D.-K. Kim, K.-M. Lee, J. Kim, M. C. Whang, and S. W. Kang, "Dynamic correlations between heart and brain rhythm during Autogenic medita- tion," *Frontiers in Human Neuroscience*, vol. 7, pp. 414–1687, 2013 Jul 31.

[45] M. Ako, T. Kawara, S. Uchida et al., "Correlation between electroencephalography and heart rate variability during sleep," *Psychiatry and Clinical Neurosciences*, vol. 57, no. 1, pp. 59–65, 2003.

[46] B. B. Green, A. J. Cook, and J. D. Ralston, "Effectiveness of home blood pressure monitoring, web communication, and pharmacist care on hypertension control: a randomized controlled trial," *Journal of the American Medical Association*, vol. 299, no. 24, pp. 2857–2867, 2008.

[47] A. L. Schneider and K. G. Jordan, "Regional Attenuation WithOut Delta (RAWOD): a distinctive EEG pattern that can aid in the diagnosis and management of severe acute ischemic stroke," *American Journal of Electroneurodiagnostic Technology*, vol. 45, no. 2, pp. 102–117, 2005.

[48] R. V. A. Sheorajpanday, G. Nagels, A. J. T. M. Weeren, M. J. A. M. van Putten, and P. P. De Deyn, "Quantitative EEG in ischemic stroke: correlation with functional status after 6months," *Clinical Neurophysiology*, vol. 122, no. 5, pp. 874–883, 2011.

[49] S. Giaquinto, A. Cobianchi, F. Macera, and G. Nolfe, "EEG recordings in the course of recovery from stroke," *Stroke*, vol. 25, no. 11, pp. 2204–2209, 1994.

[50] C. Fanciullacci, F. Bertolucci, G. Lamola et al., "Delta power is higher and more symmetrical in ischemic stroke patients with cortical involvement," *Frontiers in Human Neuroscience*, vol. 11, p. 385, 2017.

[51] R. A. L. Macdonell, G. A. Donnan, P. F. Bladin, S. F. Berkovic, and C. H. R. Wriedt, "The electroencephalogram and acute ischemic stroke: distinguishing cortical from lacunar infarction," *Archives of Neurology*, vol. 45, no. 5, p. 520, 1988.

[52] J. I. Doerrfuss, T. Kilic, M. Ahmadi, M. Holtkamp, and J. E. Weber, "Quantitative and qualitative EEG as a prediction tool for outcome and complications in acute stroke patients," *Clinical EEG and Neuroscience*, vol. 51, no. 2, pp. 121–129, 2019.

[53] A. Aminov, J. M. Rogers, S. J. Johnstone, S. Middleton, and P. H. Wilson, "Acute single channel EEG predictors of cognitive function after stroke," *PLoS One*, vol. 12, no. 10, Article ID e0185841, 2017.

[54] E. H. Wagner, B. T. Austin, and M. V. Korff, "Organizing care for patients with chronic illness," *The Milbank Quarterly*, vol. 74, no. 4, pp. 511–544, 1996.

[55] J. M. E. Walsh, K. M. McDonald, K. G. Shojania et al., "Quality improvement strategies for hypertension management: a systematic review," *Medical Care*, vol. 44, no. 7, pp. 646–657, 2006.

[56] C. Sharma, B. Amandeep, R. Sobti, T. K. Lohani, and M. Shabaz, "A Secured Frame Selection Based Video Water-Marking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption," *Security and Communication Networks*, vol. 2021, Article ID 5536170, 19 pages, 2021.

[57] M. A. Sayeed, S. P. Mohanty, E. Kougianos, and H. P. Zaveri, "eSeiz: an edge-device for accurate seizure detection for smart healthcare," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 379–387, 2019.

[58] P. Sundaravadivel, V. Goyal, and L. Tamil, "I-rise: an iot-basedsemi-immersive affective monitoring framework for anxiety disorders," in *Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–5, Las Vegas, NV, USA, November 2020.

[59] W. Meng, W. Li, D. S. Wong, and J. Z. Tmguard, "A touch movement-based security mechanism for screen unlock patterns on smartphones," *Applied Cryptography and Network Security*, vol. 9696, 2016.

[60] L. Rachakonda, S. P. Mohanty, E. Kougianos, and P. Sundaravadivel, "Stress-lysis: a DNN-integrated edge device for stress level detection in the IoMT," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 4, pp. 474–483, 2019.

[61] L. Rachakonda, P. Rajkumar, S. P. Mohanty, and E. K. imirror, "A smart mirror for stress detection in the iomt framework for advancements in smart cities," in *Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2)*, pp. 1–7, Piscataway, NJ, USA, October 2020.

[62] L. Rachakonda, S. P. Mohanty, and E. Kougianos, "ILog: an intelligent device for automatic food intake monitoring and stress detection in the IoMT," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 115–124, 2020.

[63] N. Sharma and C. Chakraborty, "Evaluation of bioinspired algorithms for image optimization," *Journal of Electronic Imaging*, vol. 31, no. 04, Article ID 041206, 2022.

[64] N. Sharma, C. Chakraborty, and R. Kumar, "Optimized multimedia data through computationally intelligent algorithms," *Multimedia Systems*, Springer Science and Business Media LLC, Berlin, Germany, pp. 1–17, 2022.

[65] N. M. Lutimath, H. V. Ramachandra, S. Raghav, and N. Sharma, "Prediction of heart disease using genetic algorithm," in *Proceedings of Second Doctoral Symposium on Computational Intelligence*, pp. 49–58, Springer, Berlin, Germany, 2022.

[66] N. Sharma and U. Batra, "An enhanced Huffman-PSO based image optimization algorithm for image steganography," *Genetic Programming and Evolvable Machines*, vol. 22, no. 2, p. 189, 2021.

[67] N. M. Lutimath, N. Sharma, and B. K. Byregowda, "Prediction of heart disease using random forest," in *Proceedings of the 2021 emerging trends in industry 4.0 (ETI 4.0)*, pp. 1–4, Raigarh, India, 2021, May.

Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 4845850, 13 pages
https://doi.org/10.1155/2023/4845850

Research Article

Provably Secure and Lightweight Patient Monitoring Protocol for Wireless Body Area Network in IoHT

Qi Xie, Dongnan Liu, Zixuan Ding, Xiao Tan, and Lidong Han

Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China

Correspondence should be addressed to Qi Xie; qixie68@126.com

Received 21 April 2022; Revised 4 June 2022; Accepted 24 November 2022; Published 13 February 2023

Academic Editor: Muhammad Asghar Khan

As one of the important applications of Internet of Health Things (IoHT) technology in the field of healthcare, wireless body area network (WBAN) has been widely used in medical therapy, and it can not only monitor and record physiological information but also transmit the data collected by sensor devices to the server in time. However, due to the unreliability and vulnerability of wireless network communication, as well as the limited storage and computing resources of sensor nodes in WBAN, a lot of authentication protocols for WBAN have been devised. In 2021, Alzahrani et al. designed an anonymous medical monitoring protocol, which uses lightweight cryptographic primitives for WBAN. However, we find that their protocol is defenseless to off-line identity guessing attacks, known-key attacks, and stolen-verifier attacks and has no perfect forward secrecy. Therefore, a patient monitoring protocol for WBAN in IoHT is proposed. We use security proof under the random oracle model (ROM) and automatic verification tool ProVerif to demonstrate that our protocol is secure. According to comparisons with related protocols, our protocol can achieve both high computational efficiency and security.

1. Introduction

Wireless body area network (WBAN) exists as a transmission network for body monitoring. It has intellectual network appliances, such as personal wireless terminals, wearable devices, and wireless sensors. Individuals can use network devices to build personalized health networks based on WBAN, and they are substantial participants in the Internet of Health Things (IoHT) application. WBAN is widely used in patient monitoring, physiological parameter measurement, and so on. The measured data are transmitted by the sensor to the devices with a forwarding function in real time using wireless network transmission and then stored in the database of the remote server [1–3]. Using WBAN-based systems, patient-specific electronic medical records can be established, and professionals can analyze medical data through patient electronic records. Moreover, the electronic data of patients can be used for later analysis and diagnosis, and medical personnel can provide targeted medical services based on these data [4].

The communication and interaction of WBAN are based on an open wireless channel, so it is inevitable to face a series of challenges. Attackers can eavesdrop, tamper, intercept publicly transmitted information, and use the obtained information to launch attacks and obtain patients' privacy. This poses a great threat to the medical IoHT and patient privacy [5, 6]. In addition, the WBAN system requires real-time data transmission and timely processing of a large number of communication requests, which makes the energy consumption of infrastructures with limited efficiency very heavy [7]. However, most devices for WBAN have limited computing power, so they cannot perform traditional cryptographic calculations. Moreover, intensive computation will bring about overblown network loads, which will affect the performance of the system. Therefore, the medical field urgently needs a lightweight privacy-protected secure key agreement to meet the above challenges.

In recent years, a lot of anonymous medical key agreements have been proposed. An innovative dynamic ID-based key agreement in telecare medical information system (TMIS) was presented by Chen et al. [8]. However, Xie et al. [9] state that Chen et al.'s scheme cannot defend against off-line password guessing attacks and impersonation attacks and has no privacy protection and perfect forward secrecy. Xie et al. [10] presented a novel authentication protocol for TMIS in 2014, which is considered to be pragmatic and secure. Radhakrishnan and Muniyandi [11] submitted a two-factor key agreement for TMIS based on elliptic curve cryptography (ECC). In 2015, Wang and Zhang [12] solved the anonymity of authentication in WBAN using bilinear pairs, and their scheme could defend against known-key attacks and man-in-middle attacks. However, according to the research of Jiang et al. [13], the protocol cannot resist client forgery attacks, is not suitable for practical applications, and may lead to nonsynchronization of system logs. In 2017, Li et al. [14] proposed an anonymous authentication scheme. It employs lightweight cryptographic primitives (e.g., hash function operations) and asserts that it has realized the mutual authentication of the sensor nodes worn by patients and the hub node and has realized unlinkability and anonymity. Later, Koya et al. [15] stated that it is not feasible because their scheme assumes that the central node is entirely credible. Moreover, it is defenseless to sensor impersonation attacks. Soni and Singh [16] submitted a lightweight authentication scheme employing low-cost operations for WBAN. Based on the wireless medical sensor network, Jan et al. [17] submitted a patient key agreement for the healthcare system to realize secure and efficient communication between users and sensors. Recently, Ullah et al. [18] submitted a hyperelliptic curve and pragmatic IoT-based crossdomain authentication scheme for WBAN. In addition, Ullah et al. [19–21] proposed a multimessage signcryption protocol, anonymous certificateless signcryption protocol, and certificate-founded signcryption protocol for IoHT. Khan et al. [22] proposed an online-offline certificate-less signature protocol for IoHT.

Wu et al. [23] designed an identity authentication scheme using unilateral bilinear pairing technology which only performs bilinear pairing at the access point (AP). After that, Chen and Peng [24] declared that it cannot realize mutual authentication and is also susceptible to client forgery attacks. Li et al. [25] devised a key agreement founded on ECC to realize user anonymity. But Sowjanya et al. [26] found that their scheme not only has the problems of clock nonsynchronization and excessive control power of users but also no perfect forward secrecy. Kalra and Sood [27] submitted a secure key agreement that is not affected by time synchronization, which is based on the password. In 2021, Chunka et al. [28] reviewed their scheme and found that it had many security issues. For instance, due to the defects in the gateway design, the scheme cannot confirm the authenticities of sensor nodes, so it cannot resist the sensor nodes captured attacks, and the gateway private key is prone to be leaked. In addition, a large number of redundant multiple hash calculations increase the computational burden on the system. Xu et al. [29] raised an anonymous and lightweight patient monitoring protocol using lightweight cryptographic primitives. The survey of Alzahrani et al. [30] shows that off-line identity guessing attacks will wreck its anonymity, and it is also defenseless to key compromise attacks and replay attacks.

1.1. Motivation and Contributions.

According to the summary of the existing literature [30–33], we found that some protocols using lightweight cryptographic primitives cannot resist various attacks, and many protocols based on asymmetric cryptography have high time complexity. In 2021, Alzahrani et al. [30] designed an anonymous medical monitoring scheme. Nevertheless, their scheme is defenseless to stolen-verifier attacks, known-key attacks, and off-line identity guessing attacks and has no perfect forward secrecy. To realize a secure and lightweight authentication protocol in WBAN systems, we propose a patient monitoring protocol. Here, our contributions are as follows:

(i) We reviewed Alzahrani et al.'s [30] protocol and analyzed its drawbacks, for example, known-key attacks, stolen-verifier attacks, and off-line identity guessing attacks

(ii) A patient monitoring protocol is proposed to realize the security and lightweight requirements of WBAN systems

(iii) Using the automated verification tool ProVerif and formal security proof in ROM, we demonstrate the proposed protocol is secure

(iv) Our protocol is relatively pragmatic and secure by performance comparison

The remaining section is constructed as follows: the system model and preliminaries are given in Section 2. In Section 3, we describe the review and drawbacks of Alzahrani et al.'s protocol. Section 4 proposes a patient monitoring scheme. Its security is analyzed in Sections 5 and 6. Its security properties, computation cost, storage cost, and communication cost between ours and some related protocols are evaluated in Section 7. Section 8 concludes the paper.

2. System Model and Preliminaries

In this section, we present the system model and attack model. Concurrently, we describe the physically unclonable function (PUF).

2.1. System Model.

Figure 1 illustrates its system model. It adopts the centralized two-hop architecture of WBAN, which includes the following devices: sensor nodes (SNs), relay nodes (RNs), and medical server node (MS). RN is the intermediate node, and only needs to forward messages between SN and MS, and it can add or delete its identity before forwarding messages. RN is always within the communication coverage of MS, and SN is covered by at least one RN. Resource-constrained SN monitors and collects patients' medical health data by being worn or embedded into patients.

2.2. Attack Model.

Presuming the attacker (AR) maintains the following capacities:

(1) AR can capture messages transmitted via open channels and may eavesdrop, replace, replay, or intercept the data in these messages

(2) AR can obtain verifier table stored in MS, but cannot obtain its secret key

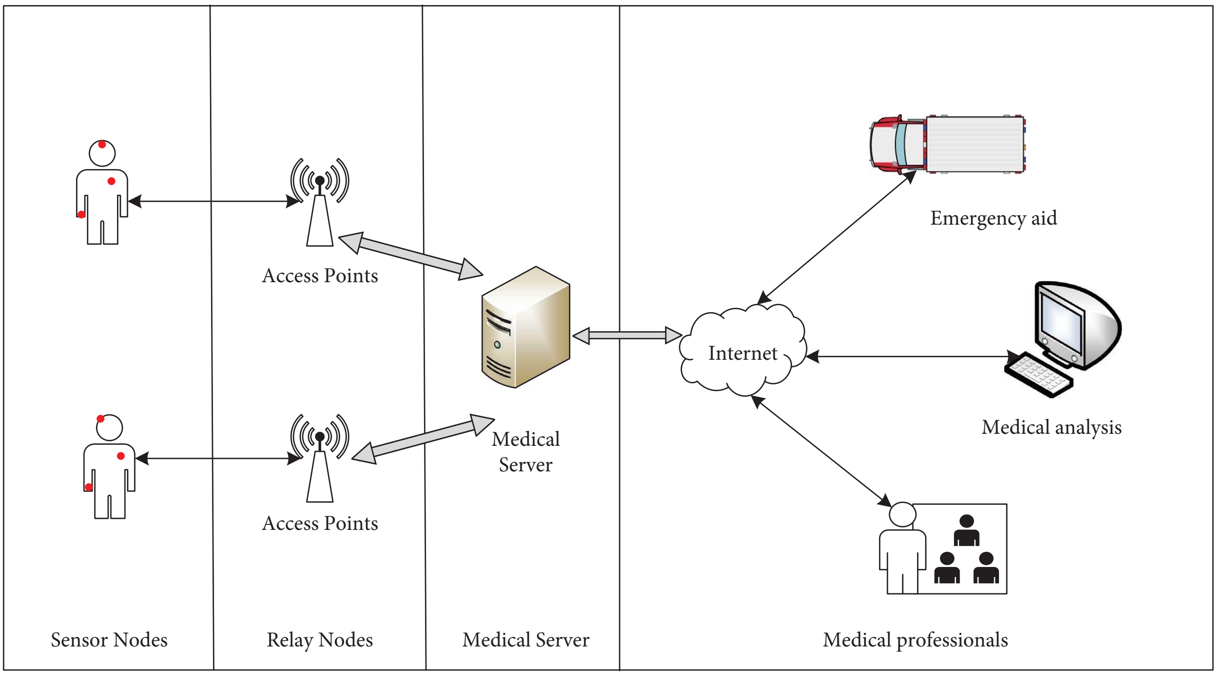


Figure 1: System model.

(3) AR can capture SN_j and RN and then retrieve all data stored in their memory

(4) We adopt Dolev–Yao threat model [34] and assume that the public channel is insecure

2.3. Physically Unclonable Function. As a hardware security technology, a physically unclonable function (PUF) can be regarded as the “digital fingerprint” of the chip [35]. It uses the inherent physical differences to produce a specific unclonable response to a given challenge. Therefore, it is difficult to be predicted before production and cloned after production. It has broad application prospects in the field of security. According to the same challenge, the response of PUF can remain unchanged under different conditions. Any detection or observation of PUF will change the circuit characteristics, and the output of PUF will also change. Therefore, PUF is often used to protect crucial data in cryptography [36].

All notations in our paper are illustrated in Table 1.

3. Drawbacks of Alzahrani et al.’s Scheme

3.1. Review of Alzahrani et al.’s Scheme. We briefly review Alzahrani et al.’s [30] anonymous authentication protocol, which involves three steps: (1) system initialization; (2) device registration; (3) mutual authentication and key agreement. SA performs step (1) and step (2) through a private channel as follows.

3.1.1. System Initialization

(i) SA generates a long-term master secret key K_{MS} for MS

(ii) Subsequently, MS reserves the master secret key K_{MS}

Table 1: Notations.

Notations	Description
SN_j	j^{th} sensor node
RN	Relay node
MS	Medical server node
SA	Server administrator
AR	The adversary
id_j, id_R	Identity of SN_j/identity of RN
K_{MS}, Q	Secret key and public key of MS, where $Q = K_{MS} \bullet P$
K_{SH}	Session key
r, P_{R1}, P_{R2}	Random integers
b_j	Random number generated by SN_j
m, r^{new}	Random integers generated by MS
a_j, r, P_{R1}, P_{R2}	Random integers generated by SA
T, T_1, T_2, T_3, T_4	Timestamps
P	The base point of the elliptic curve
$\oplus$	XOR operation
PUF$(\bullet)$	Physically unclonable function
$h(\bullet)$	Hash function
ΔT	The maximum transmission delay

3.1.2. Devices Registration

(i) SA selects three random integers r, P_{R1}, P_{R2}, and an identity id_j for the sensor node SN_j and reserves tuple $<id_j, P_{R1}, P_{R2}>$ in the memory of MS

(ii) SA computes $x_{Nj} = r \oplus K_{MS}$, $y_{Nj} = id_j \oplus h(K_{MS}, r)$

(iii) SA reserves tuple $<id_j, x_{Nj}, y_{Nj}, P_{R1}, P_{R2}>$ in the memory of SN_j

(iv) Finally, the verification table of MS is $<id_j, P_{R1}, P_{R2}, id_R>$

3.1.3. Mutual Authentication and Key Agreement. The communications between SN_j and MS are as follows:

(i) SN_j creates a current timestamp T_1 and computes the validation $Vid_j = h(id_j, x_{Nj}, y_{Nj}, P_{R2}, T_1)$, where id_j is SN_j's identity, $x_{Nj} = r \oplus K_{MS}$, $y_{Nj} = id_j \oplus h(K_{MS}, r)$, P_{R2} denotes a random integer, and the current timestamp is denoted as T_1.

(ii) SN_j submits Message1 tuple $<x_{Nj}, y_{Nj}, Vid_j, T_1>$ to RN.

(iii) RN appends its identity id_R and forwards the Message2 tuple $<x_{Nj}, y_{Nj}, Vid_j, T_1, id_R>$ to MS.

(iv) MS scans the identity id_R and finishes the session if no record is found in its memory. Otherwise, MS creates the current timestamp T_2 and checks if $|T_2 - T_1| \leq \Delta T$, and if not, finishes the session. Otherwise, MS computes $r^* = x_{Nj} \oplus K_{MS}$, $id_j^* = y_{Nj} \oplus h(K_{MS}, r^*)$. MS checks the validity of the identity id_j^*, if so, MS extracts the tuple $<id_j^*, P_{R1}, P_{R2}>$ from its memory, computes $Vid_j^* = h(id_j^*, x_{Nj}, y_{Nj}, P_{R2}, T_1)$, and checks $Vid_j^* ? = Vid_j$. If so, MS generates random nonce m and r^{new} and computes $s = id_j^* \oplus y_{Nj}$, $j = id_j^* \oplus x_{Nj}$, $v = m \oplus s$, $x_{Nj}^{\text{new}} = r^{\text{new}} \oplus K_{MS}$, $y_{Nj}^{\text{new}} = id_j^* \oplus h(K_{MS}, r^{\text{new}})$, $g = h(m, s, j, P_{R2})$, $u = x_{Nj}^{\text{new}} \oplus g$, $n = y_{Nj}^{\text{new}} \oplus g$, $\Delta = h(m, id_j^*, s, x_{Nj}^{\text{new}}, y_{Nj}^{\text{new}})$, and the session key $K_{SH} = h(m, j, P_{R1}, P_{R2})$. Afterwards, MS sends the Message3 tuple $<v, u, \Delta, n, id_R>$ to RN. MS displaces P_{R1} with P_{R2} and P_{R2} with K_{SH}.

(v) RN removes its identity id_R and forwards the Message 4 tuple $<v, u, \Delta, n>$ to SN_j.

(vi) SN_j computes $s^* = id_j \oplus y_{Nj}$, $m^* = v \oplus s^*$, $j^* = id_j \oplus x_{Nj}$, $g^* = h(m^*, s^*, j^* P_{R2})$, $x_{Nj}^{\text{new+}} = u \oplus g^*$, $y_{Nj}^{\text{new+}} = n \oplus g^*$, $\Delta^* = h(m^*, id_j, s^*, x_{Nj}^{\text{new+}}, y_{Nj}^{\text{new+}})$. Afterwards, SN_j checks $\Delta^* ? = \Delta$. If so, SN_j computes the session key $K_{SH} = h(m^*, j^*, P_{R1}, P_{R2})$. SN_j displaces x_{Nj} and y_{Nj}, with $x_{Nj}^{\text{new+}}$ and $y_{Nj}^{\text{new+}}$, and stores them in its memory. Finally, SN_j displaces P_{R1} with P_{R2} and P_{R2} with K_{SH}.

3.2. Drawbacks

3.2.1. Off-Line Identity Guessing Attack. Supposing an adversary (AR) can eavesdrop on the conversation between SN_j and MS. AR intercepts the first round of x_{Nj-1}, y_{Nj-1}, and the second round of x_{Nj-2}, y_{Nj-2}, where x_{Nj-2} and y_{Nj-2} are the first round of $x_{Nj-1}^{\text{new+}}$ and $y_{Nj-1}^{\text{new+}}$. AR computes $\Delta^* = h(m^*, id_j, s^*, x_{Nj-1}^{\text{new+}}, y_{Nj-1}^{\text{new+}})$, where $m^* = v \oplus s^*$, $s^* = id_j \oplus y_{Nj}$. Only id_j in Δ^* is unknown, and AR guesses id_j to verify if $\Delta^* ? = \Delta$. If so, AR obtains id_j successfully. Otherwise, guesses id_j again.

3.2.2. Desynchronization Attack. If AR intercepts Message4 and drops it, the SN_j will miss it. The insecurity is that MS has updated x_{Nj}, y_{Nj}, P_{R1}, P_{R2}, but SN_j has not. This will make every subsequent authentication process between SN_j and MS fail.

3.2.3. Stolen-Verifier Attack. If the verifier table $<id_j$, P_{R1}, P_{R2}, $id_R>$ of MS is stolen, AR can obtain all the data in it. AR eavesdrops on the communication between SN_j and MS, intercepts Message1 tuple $<x_{Nj}, y_{Nj}, Vid_j, T_1>$, Message 4 tuple $<v, u, \Delta, n>$, computes $s^* = id_j \oplus y_{Nj}$, $m^* = v \oplus s^*$, and $j^* = id_j \oplus x_{Nj}$, and computes the session key $K_{SH} = h(m^*, j^*, P_{R1}, P_{R2})$. That is, AR can obtain the session key.

3.2.4. Known-Key Attack. If the session keys of two consecutive rounds are leaked, AR will get P_{R1-3} and P_{R2-3} of the third round. According to identity guessing attacks, AR obtains the SN's identity id_j. In the third round of protocol execution, AR intercepts message 1 and message 4 and computes $s^* = id_j \oplus y_{Nj-3}$, $m^* = v \oplus s^*$, $g^* = h(m^*, s^*, j^* P_{R2-3})$, $x_{Nj-3}^{\text{new+}} = u \oplus g^*$, $y_{Nj-3}^{\text{new+}} = n \oplus g^*$, $K_{SH} = h(m^*, j^*, P_{R1-3}, P_{R2-3})$. Therefore, the session key of the subsequent round will be obtained by the AR.

3.2.5. No Perfect Forward Security. If the long-term secret key K_{MS} and short-term secret key P_{R1} and P_{R2} of the Alzahrani et al.'s [30] scheme are leaked, AR calculates $r^* = x_{Nj} \oplus K_{MS}$, $id_j = y_{Nj} \oplus h(K_{MS}, r^*)$. Then, AR calculates $s^* = id_j \oplus y_{Nj}$, $m^* = v \oplus s^*$, $g^* = h(m^*, s^*, j^*, P_{R2})$. Finally, AR can compute the session key $K_{SH} = h(m^*, j^*, P_{R1}, P_{R2})$. Therefore, it doesn't achieve perfect forward secrecy.

4. Proposed Protocol

A security-enhanced protocol is presented, which involves three steps: (1) system initialization; (2) device registration; (3) mutual authentication and key agreement. SA executes initialization and registration steps through a private channel as follows.

4.1. Initialization. SA executes as follows:

(1) The master secret key K_{MS} is generated by SA

(2) Subsequently, MS accepts the master secret key K_{MS} via a secure channel and keeps it secretly

(3) SA chooses an elliptic curve $E_c(\alpha, \beta)$ of large order. P is a base point. SA computes $Q = K_{MS} \bullet P$. Afterwards, SA chooses a hash function $h(\bullet)$.

4.2. Registration. The registration phase can be described as follows:

(1) SA chooses the random integer a_j and the identity id_j for the sensor node SN_j, an identity id_R for RN, and reserves id_j and id_R in the memory of MS

(2) SA computes $x_{Nj} = a_j \oplus h(K_{MS}, T_j)$, $y_{Nj} = id_j \oplus h(K_{MS}, a_j, T_j)$, $MH_j = h(id_j, K_{MS})$, where T_j is the current timestamp, and K_{MS} is MS's secret key

(3) SA reserves the tuple $<id_j, x_{Nj}, y_{Nj}, MH_j, T_j>$ in the memory of SN_j, and SN_j generates a challenge Cha_j and computes $\mathrm{Res}_j = \mathrm{PUF}(\mathrm{Cha}_j)$, $ST_j = h(\mathrm{Res_j}) \oplus MH_j$, where PUF is deployed in the sensor node SN_j

(4) Finally, SN_j stores $\{id_j, x_{Nj}, y_{Nj}, \mathrm{ST_j}, \mathrm{Cha_j}, \mathrm{T_j}\}$, and the verification table of MS is $\{id_R, id_j\}$

4.3. Mutual Authentication and Key Agreement. This phase is shown in Figure 2.

(1) SN_j chooses the random integer b_j and the timestamp T_1 and calculates $MH_j = h(\mathrm{PUF}(\mathrm{Cha}_j)) \oplus ST_j$, $A_1 = b_j \bullet P$, $A_2 = b_j \bullet Q$, $Vid_j = h(id_j, x_{Nj}, y_{Nj}, A_1, A_2, h(A_2, MH_j), T_j, T_1)$.

(2) SN_j submits the Message1 tuple $<x_{Nj}, y_{Nj}, Vid_j, A_1, T_j, T_1>$ to RN.

(3) RN appends its identity id_R and forwards the Message 2 tuple $<x_{Nj}, y_{Nj}, Vid_j, A_1, T_j, T_1, id_R>$ to MS.

(4) MS scans the identity id_R and finishes the session if no record is found in its memory. Otherwise, MS creates the current timestamp T_2 and checks if $|T_2 - T_1| \le \Delta T$, and if not, finishes the session. Otherwise, MS computes $a_j = x_{Nj} \oplus h(K_{MS}, T_j)$, $id_j^* = x_{Nj} \oplus h(K_{MS}, a_j, T_j)$. MS calculates $A_2^* = K_{MS} \bullet A_1$, $Vid_j^* = h(id_j^*, x_{Nj}, y_{Nj}, A_1, A_2^*, h(A_2^*, h(id_j^*, K_{MS})), T_j, T_1)$ and checks $Vid_j^* ?= Vid_j$. If so, MS creates random numbers a_i and b_i. Next, MS computes $A_3 = b_i \bullet P$, $A_4 = b_i \bullet A_1$, $x_{Nj}^{\mathrm{new}} = a_i \oplus h(K_{MS}, T_2)$, $y_{Nj}^{\mathrm{new}} = id_j^* \oplus h(K_{MS}, a_i, T_2)$, $\mu = x_{Nj}^{\mathrm{new}} \oplus h(A_2^*, h(id_j^*, K_{MS}), T_2)$, $\lambda = y_{Nj}^{\mathrm{new}} \oplus h(T_2, A_2^*, h(id_j^*, K_{MS}))$, the session key $K_{SH} = h(A_1, A_2^*, A_3, A_4, id_j^*, T_2)$, and $\Delta = h(x_{Nj}^{\mathrm{new}}, y_{Nj}^{\mathrm{new}}, K_{SH}, T_2)$. Afterwards, MS sends the Message3 tuple $<\mu, \lambda, \Delta, A_3, T_2, id_R>$ to RN.

(5) RN removes its identity id_R and forwards the Message4 tuple $<\mu, \lambda, \Delta, A_3, T_2>$ to SN_j.

(6) SN_j creates the current timestamp T_3 and checks if $|T_3 - T_2| \le \Delta T$, and if not, finishes the session. Otherwise, SN_j computes $A_4^* = b_j \bullet A_3$, $x_{Nj}^{\mathrm{new}*} = \mu \oplus h(A_2, MH_j, T_2)$, $y_{Nj}^{\mathrm{new}*} = \lambda \oplus h(T_2, A_2, MH_j)$, $K_{SH} = h(A_1, A_2, A_3, A_4^*, id_j, T_2)$, $\Delta^* = h(x_{Nj}^{\mathrm{new}*}, y_{Nj}^{\mathrm{new}*}, K_{SH}, T_2)$. SN_j checks if $\Delta^* ?= \Delta$. If so, SN_j successfully establishes the session key K_{SH} with MS and updates $<x_{Nj}, y_{Nj}, \mathrm{T_j}>$ with $<x_{Nj}^{\mathrm{new}*}, y_{Nj}^{\mathrm{new}*}, T_2>$.

5. Informal Security Analysis

5.1. Off-Line Identity Guessing Attack. If an adversary(AR) can eavesdrop on the open channel and guess id_j of the sensor node $\mathrm{SN_j}$, it is not feasible for him/her to verify whether $Vid_j^* ?= Vid_j$ is correct or not without knowing A_2, where $A_2 = b_j \bullet K_{MS} \bullet P$, $Vid_j = h(id_j, x_{Nj}, y_{Nj}, A_1, A_2, h(A_2, MH_j), T_j, T_1)$, $MH_j = h(id_j, K_{MS})$. Because of computational Diffie–Hellman problem (CDHP), AR cannot compute $A_2 = b_j \bullet K_{MS} \bullet P$ from $A_1 = b_j \bullet P$ and $Q = K_{MS} \bullet P$. Therefore, off-line identity guessing attack is infeasible.

5.2. Desynchronization Attack. In the improved protocol, x_{Nj} and y_{Nj} are updated as x_{Nj}^{new} and y_{Nj}^{new} on the side of the MS. Even if AR intercepts the Message4, it has no impact on the next session between the sensor node SN_j and the MS.

5.3. Stolen-Verifier Attack. Stolen-verifier attack means that an adversary can obtain verification table except the secret key from MS by trespassing on the device or side channel attack and then launch attacks. In the proposed scheme, the verification table of MS only contains the identities id_j and id_R of SN_j and RN. So the adversary cannot launch any attacks even if he or she obtains these identities. Thus, the protocol defends against stolen-verifier attacks.

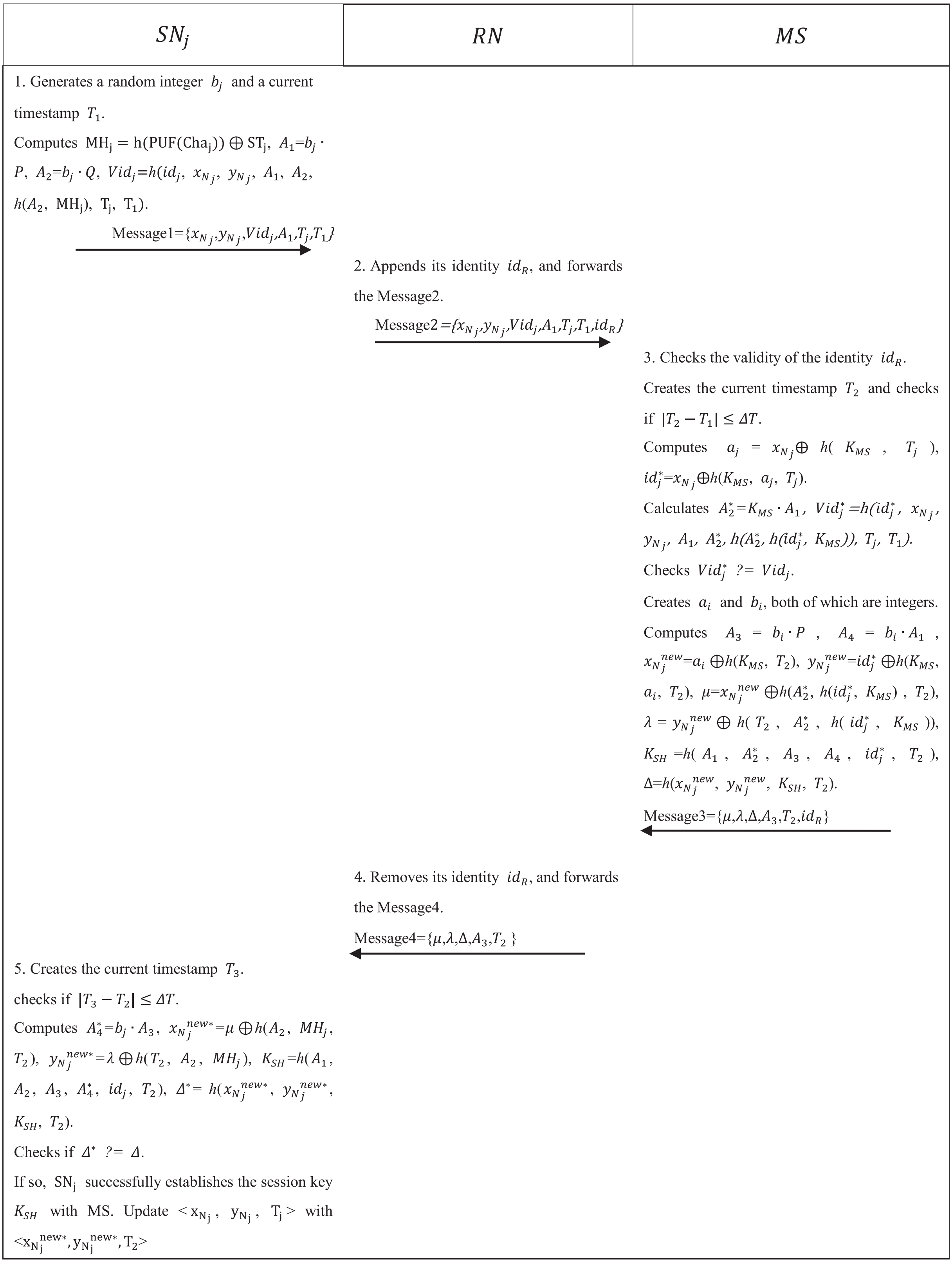
5.4. Known-Key Attack. Assuming that AR knows the session key $K_{SH} = h(A_1, A_2, A_3, A_4^*, id_j, T_2)$, because K_{SH} only contained in $\Delta^* = h(x_{Nj}^{\mathrm{new}*}, y_{Nj}^{\mathrm{new}*}, K_{SH}, T_2)$, so AR cannot launch any attack.

5.5. Smart Card Lost Attack. By the side-channel attack, AR is able to get all data reserved in the smart card when it is lost, and then launch attacks. However, in our protocol, smart card isn't used, so the protocol defends against the smart card lost attack.

5.6. Sensor Node Captured Attack. In the improved protocol, the sensor node SN_j stores $\{id_j, x_{Nj}, y_{Nj}, ST_j, \mathrm{Cha}_j, T_j\}$, where id_j is SN_1's identity, $x_{Nj} = a_j \oplus h(K_{MS}, T_j)$, $y_{Nj} \oplus id_j \oplus h(K_{MS}, a_j, T_j)$, $ST_j = h(\mathrm{PUF}(\mathrm{Cha}_j)) \oplus MH_j$, Cha_j is the challenge of PUF, T_j is the timestamp, and K_{MS} is the secret key of MS. Assuming that the sensor node SN_j is captured by AR, he/she cannot obtain the secret parameter MH_j to impersonate SN_j because of PUF. In addition, AR cannot obtain the secret key K_{MS}. Therefore, the sensor node captured attack cannot influence the security of nodes and the sensor network.

5.7. Anonymity and Unlinkability. The identity id_j of the sensor node SN_j is in Message 1 $= \{x_{Nj}, y_{Nj}, Vid_j, A_1, T_j, T_1\}$ and transmitted via an open channel, where $Vid_j = h(id_j, x_{Nj}, y_{Nj}, A_1, A_2, h(A_2, MH_j)T_j, T_1)$, $MH_j = h(id_j, K_{MS})$, $y_{Nj} = id_j \oplus h(K_{MS}, a_j, T_j)$. So an adversary cannot compute the identity id_j of the sensor SN_j because he can not know the secret key K_{MS} of MS. Thus, our scheme achieves anonymity. Moreover, because each session will generate new b_j and T_j, the identity id_j of the sensor node SN_j cannot be tracked by AR.

5.8. Perfect Forward Secrecy. If AR obtains all the secret information of the sensor node SN_j and the long-term master secret key K_{MS} of MS, because of CDHP, he/she still



SN_j

RN

MS

1. Generates a random integer b_j and a current timestamp T_1.
Computes $\mathrm{MH_j} = \mathrm{h(PUF(Cha_j))} \oplus \mathrm{ST_j}$, $A_1{=}b_j \cdot P$, $A_2{=}b_j \cdot Q$, $Vid_j{=}h(id_j,\ x_{N_j},\ y_{N_j},\ A_1,\ A_2,\ h(A_2,\ \mathrm{MH_j}),\ \mathrm{T_j},\ \mathrm{T_1})$.

Message1=$\{x_{N_j}, y_{N_j}, Vid_j, A_1, T_j, T_1\}$

2. Appends its identity id_R, and forwards the Message2.

Message2=$\{x_{N_j}, y_{N_j}, Vid_j, A_1, T_j, T_1, id_R\}$

3. Checks the validity of the identity id_R.
Creates the current timestamp T_2 and checks if $|T_2 - T_1| \leq \Delta T$.
Computes $a_j = x_{N_j} \oplus h(K_{MS},\ T_j)$, $id_j^*{=}x_{N_j} \oplus h(K_{MS},\ a_j,\ T_j)$.
Calculates $A_2^*{=}K_{MS} \cdot A_1$, $Vid_j^*{=}h(id_j^*,\ x_{N_j},\ y_{N_j},\ A_1,\ A_2^*,\ h(A_2^*,\ h(id_j^*,\ K_{MS})),\ T_j,\ T_1)$.
Checks $Vid_j^*\ ?{=}\ Vid_j$.
Creates a_i and b_i, both of which are integers.
Computes $A_3 = b_i \cdot P$, $A_4 = b_i \cdot A_1$, $x_{N_j}^{new}{=}a_i \oplus h(K_{MS},\ T_2)$, $y_{N_j}^{new}{=}id_j^* \oplus h(K_{MS},\ a_i,\ T_2)$, $\mu{=}x_{N_j}^{new} \oplus h(A_2^*,\ h(id_j^*,\ K_{MS}),\ T_2)$, $\lambda = y_{N_j}^{new} \oplus h(T_2,\ A_2^*,\ h(id_j^*,\ K_{MS}))$, $K_{SH}{=}h(A_1,\ A_2^*,\ A_3,\ A_4,\ id_j^*,\ T_2)$, $\Delta{=}h(x_{N_j}^{new},\ y_{N_j}^{new},\ K_{SH},\ T_2)$.

Message3=$\{\mu, \lambda, \Delta, A_3, T_2, id_R\}$

4. Removes its identity id_R, and forwards the Message4.

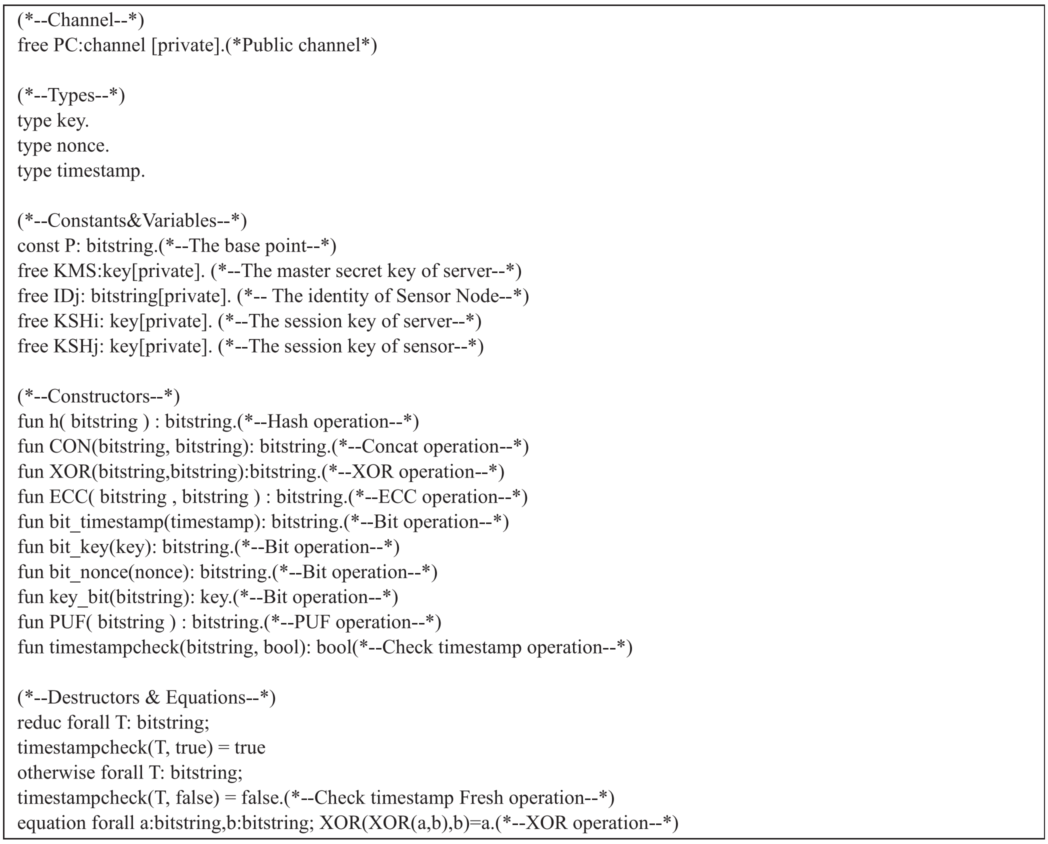
Message4=$\{\mu, \lambda, \Delta, A_3, T_2\}$

5. Creates the current timestamp T_3.
checks if $|T_3 - T_2| \leq \Delta T$.
Computes $A_4^*{=}b_j \cdot A_3$, $x_{N_j}^{new*}{=}\mu \oplus h(A_2,\ MH_j,\ T_2)$, $y_{N_j}^{new*}{=}\lambda \oplus h(T_2,\ A_2,\ MH_j)$, $K_{SH}{=}h(A_1,\ A_2,\ A_3,\ A_4^*,\ id_j,\ T_2)$, $\Delta^*{=}\ h(x_{N_j}^{new*},\ y_{N_j}^{new*},\ K_{SH},\ T_2)$.
Checks if $\Delta^*\ ?{=}\ \Delta$.
If so, $\mathrm{SN_j}$ successfully establishes the session key K_{SH} with MS. Update $<\mathrm{x_{N_j}},\ \mathrm{y_{N_j}},\ \mathrm{T_j}>$ with $<\mathrm{x_{N_j}^{new*}}, \mathrm{y_{N_j}^{new*}}, \mathrm{T_2}>$

Figure 2: Mutual authentication and key agreement phase.

cannot successfully calculate $K_{SH} = h(A_1, A_2, A_3, A_4^*, id_j, T_2)$ without knowing A_4^*. Therefore, the protocol achieves perfect forward secrecy.

5.9. Impersonation Attack. This attack means that AR can impersonate a legal user to generate and send a message, and the message can be passed through the authentication by the



```
(*--Channel--*)
free PC:channel [private].(*Public channel*)

(*--Types--*)
type key.
type nonce.
type timestamp.

(*--Constants&Variables--*)
const P: bitstring.(*--The base point--*)
free KMS:key[private]. (*--The master secret key of server--*)
free IDj: bitstring[private]. (*-- The identity of Sensor Node--*)
free KSHi: key[private]. (*--The session key of server--*)
free KSHj: key[private]. (*--The session key of sensor--*)

(*--Constructors--*)
fun h( bitstring ) : bitstring.(*--Hash operation--*)
fun CON(bitstring, bitstring): bitstring.(*--Concat operation--*)
fun XOR(bitstring,bitstring):bitstring.(*--XOR operation--*)
fun ECC( bitstring , bitstring ) : bitstring.(*--ECC operation--*)
fun bit_timestamp(timestamp): bitstring.(*--Bit operation--*)
fun bit_key(key): bitstring.(*--Bit operation--*)
fun bit_nonce(nonce): bitstring.(*--Bit operation--*)
fun key_bit(bitstring): key.(*--Bit operation--*)
fun PUF( bitstring ) : bitstring.(*--PUF operation--*)
fun timestampcheck(bitstring, bool): bool(*--Check timestamp operation--*)

(*--Destructors & Equations--*)
reduc forall T: bitstring;
timestampcheck(T, true) = true
otherwise forall T: bitstring;
timestampcheck(T, false) = false.(*--Check timestamp Fresh operation--*)
equation forall a:bitstring,b:bitstring; XOR(XOR(a,b),b)=a.(*--XOR operation--*)
```

Figure 3: Definitions.

receiver. That is to say, the receiver confirms that the message is initiated by a legitimate user. In our protocol, AR impersonates the sensor node SN_j to generate and send $\{x_{Nj}, y_{Nj}, Vid_j, A_1, T_j, T_1\}$ to RN, where $x_{Nj} = a_j \oplus h(K_{MS}, T_j)$, $y_{Nj} = id_j \oplus h(K_{MS}, a_j, T_j)$, $Vid_j = h(id_j, x_{Nj}, y_{Nj}, A_1, A_2, h(A_2, MH_j)T_j, T_1)$, K_{MS} is MS's secret key, and T_1 is the timestamp. The adversary cannot forge x_{Nj} and y_{Nj} without knowing K_{MS}. On the other hand, the adversary cannot compute MH_j even if he/she can obtain all data stored in MH_j due to the property of PUF. Therefore, the adversary cannot generate the valid Vid_j.

5.10. Replay Attack. If AR can obtain a message and replay it to the receiver, the message can be passed through the authentication of the receiver. In the proposed scheme, the timestamps and random nonce are used, so the protocol defends against the replay attack.

6. Formal Security Analysis

6.1. Formal Verification Using ProVerif. As an automated verification cryptographic scheme tool, ProVerif [37] is founded on the Dolev–Yao model and Prolog language. It verifies many cryptographic primitives, for example, public-key cryptography, hash function, and equations. When using ProVerif tool for verifying insecure cryptographic protocols, the tool will give a corresponding attack sequence.

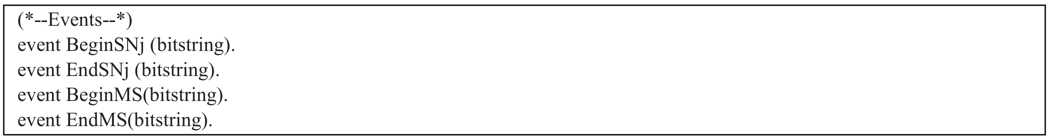
The open channel, types, constants, variables, constructors, and destructors of our proposed protocol are represented in Figure 3. We designed four events for the improved protocol, which are BeginSNj(), BeginMS(), EndSNj(), and EndMS() as depicted in Figure 4. BeginSNj() represents that the sensor node SN_j begins the key agreement session with MS. BeginMS() represents that MS starts the key agreement session with SN_j. SN_j successfully established a session key with MS, which is indicated as EndSNj(). EndMS() represents MS successfully established a session key with the sensor node SN_j.

Queries are shown in Figure 5. Figures 6 and 7 are exhibiting the processes of the sensor node $\mathrm{SN_j}$ and MS. The main process is represented in Figure 8.

For testifying the improved scheme's correctness, we propose some queries and finally implement them through simulation, as shown in Figure 9.

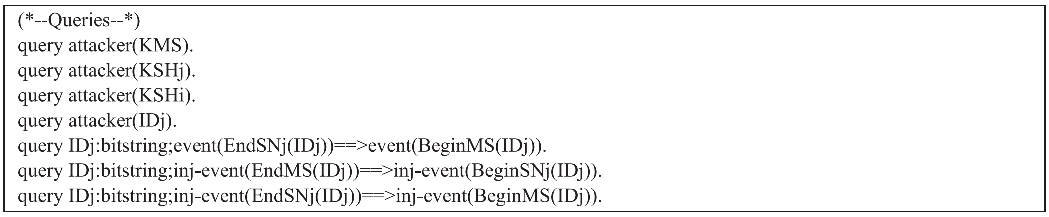
Results (1)–(4) proved that the secret parameters and session key are secure, and sensor nodes are anonymous in our protocol. Results (5)-(7) showed that the two processes began and terminated successfully in sequence.

6.2. Formal Security Proof. After identifying the random oracle model (ROM), we calculate the advantage of breaking our protocol $\mathscr{P}$ by the adversary A. The notions of ROM are clarified as follows.



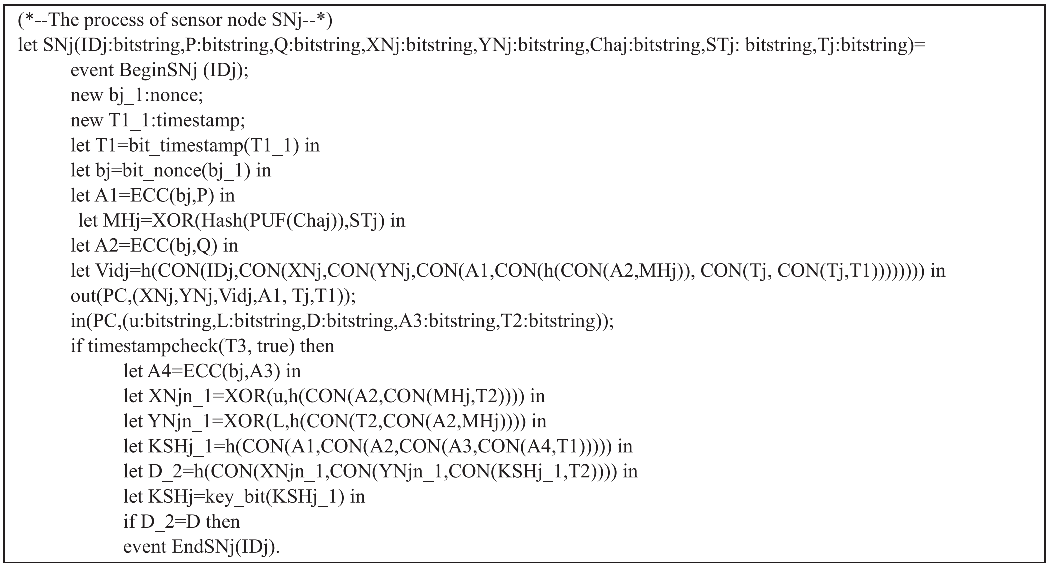
```
(*--Events--*)
event BeginSNj (bitstring).
event EndSNj (bitstring).
event BeginMS(bitstring).
event EndMS(bitstring).
```

Figure 4: Events.



```
(*--Queries--*)
query attacker(KMS).
query attacker(KSHj).
query attacker(KSHi).
query attacker(IDj).
query IDj:bitstring;event(EndSNj(IDj))==>event(BeginMS(IDj)).
query IDj:bitstring;inj-event(EndMS(IDj))==>inj-event(BeginSNj(IDj)).
query IDj:bitstring;inj-event(EndSNj(IDj))==>inj-event(BeginMS(IDj)).
```

Figure 5: Queries.



```
(*--The process of sensor node SNj--*)
let SNj(IDj:bitstring,P:bitstring,Q:bitstring,XNj:bitstring,YNj:bitstring,Chaj:bitstring,STj: bitstring,Tj:bitstring)=
        event BeginSNj (IDj);
        new bj_1:nonce;
        new T1_1:timestamp;
        let T1=bit_timestamp(T1_1) in
        let bj=bit_nonce(bj_1) in
        let A1=ECC(bj,P) in
         let MHj=XOR(Hash(PUF(Chaj)),STj) in
        let A2=ECC(bj,Q) in
        let Vidj=h(CON(IDj,CON(XNj,CON(YNj,CON(A1,CON(h(CON(A2,MHj)), CON(Tj, CON(Tj,T1)))))))) in
        out(PC,(XNj,YNj,Vidj,A1, Tj,T1));
        in(PC,(u:bitstring,L:bitstring,D:bitstring,A3:bitstring,T2:bitstring));
        if timestampcheck(T3, true) then
                let A4=ECC(bj,A3) in
                let XNjn_1=XOR(u,h(CON(A2,CON(MHj,T2)))) in
                let YNjn_1=XOR(L,h(CON(T2,CON(A2,MHj)))) in
                let KSHj_1=h(CON(A1,CON(A2,CON(A3,CON(A4,T1))))) in
                let D_2=h(CON(XNjn_1,CON(YNjn_1,CON(KSHj_1,T2)))) in
                let KSHj=key_bit(KSHj_1) in
                if D_2=D then
                event EndSNj(IDj).
```

Figure 6: The process of the sensor node $\mathbf{SN_j}$.

6.2.1. Participants & States. Three participants P is in $\mathscr{P}$, sensor node SN, relay node RN, and medical server node MS. In *i-th* instance, P, SN, RN, and MS are recorded as INS_P^i, INS_{SN}^i, INS_{RN}^i, and INS_{MS}^i, respectively. The oracles in ROM have only three states: Accept, Reject, and ⊥. Accept represents a correct message that is received by an oracle. If the message is illegal, the oracle in Reject. ⊥ means both the conditions above have not occurred.

If the oracle $\text{INS}_{SN}^i\,(\text{INS}_{MS}^i)$ is in Accept, and the session key $K_{SN}^i\,(K_{MS}^i)$ has been agreed with $\text{INS}_{MS}^i\,(\text{INS}_{SN}^i)$, then $\text{INS}_{SN}^i\,(\text{INS}_{MS}^i)$ gets the session identity $\text{SID}_{SN}^i\,(\text{SID}_{MS}^i)$, and its participant's identity is $\text{PID}_{SN}^i\,(\text{PID}_{MS}^i)$.

6.2.2. Partnering. If INS_{SN}^i and INS_{MS}^i are in Accept, the session key is negotiated. Two partners meet below requirements:

(1) $K_{SN}^i = K_{MS}^i$

(2) $\text{SID}_{SN}^i = \text{SID}_{MS}^i$

(3) $\text{PID}_{SN}^i = \text{INS}_{MS}^i$, $\text{PID}_{MS}^i = \text{INS}_{SN}^i$

6.2.3. Queries. Queries can emulate multiple attacks.

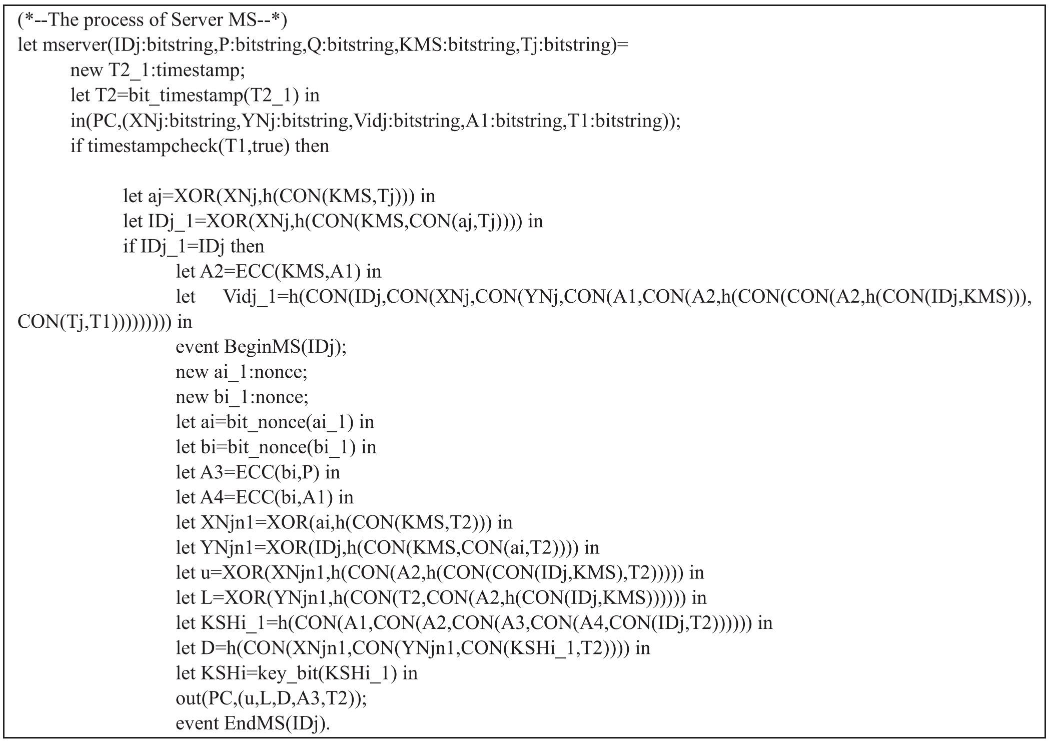
Execute(INS_P^i)if the query is lunched by A, he/she gets all the transcripts.

Send (INS_P^i, *Message*): which simulates that *Message* is sent to INS_P^i. If the message is correct, INS_P^i responses A, else, the message is ignored.

Reveal$(\text{INS}_{SN}^i, \text{INS}_{MS}^i)$if INS_{SN}^i and INS_{MS}^i are in the state Accept, the session key has been agreed, and the query *Test* has not been executed yet. Then, the session key will be revealed by this query. Else, return null.

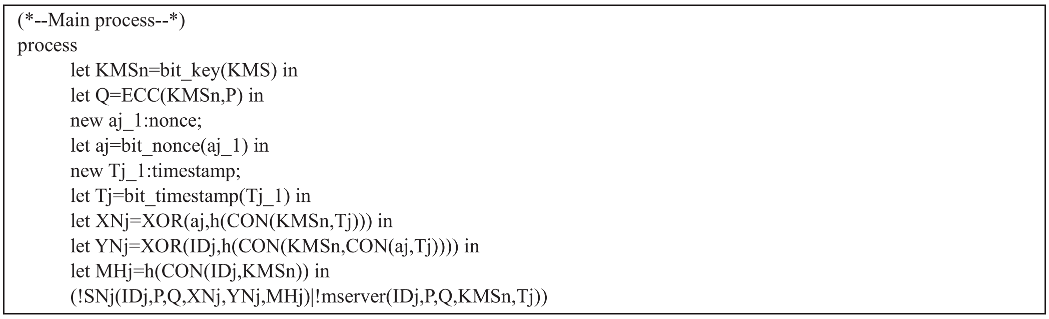
Corrupt(INS_{SN}^i)which simulates the attack of intercepting SN_j and returns the stored information $\{id_j, x_{Nj}, y_{Nj}, ST_j, \text{Cha}_j, \text{PUF}, T_j\}$ in it.

Test(INS_{SN}^i)this query produces a random bit r, which is performed no more than once. If $r = 1$ and the session key has been agreed, the real session key is returned to A, else, the query returns a random session key.



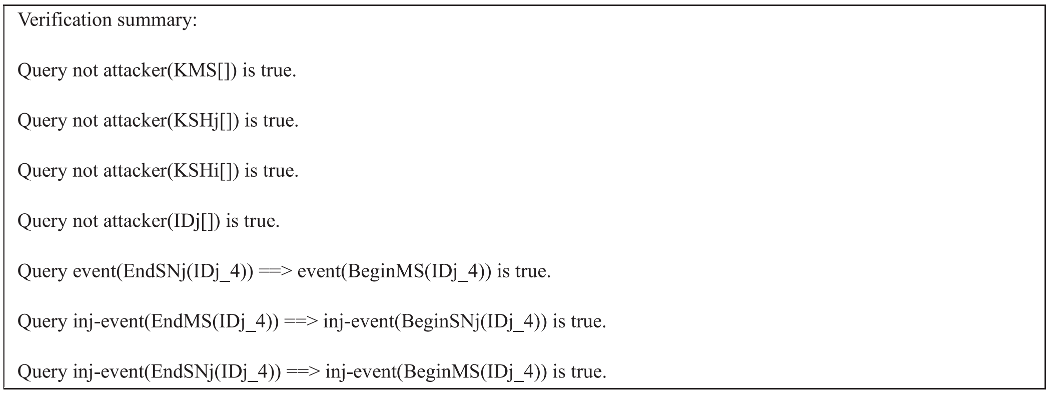
```
(*--The process of Server MS--*)
let mserver(IDj:bitstring,P:bitstring,Q:bitstring,KMS:bitstring,Tj:bitstring)=
        new T2_1:timestamp;
        let T2=bit_timestamp(T2_1) in
        in(PC,(XNj:bitstring,YNj:bitstring,Vidj:bitstring,A1:bitstring,T1:bitstring));
        if timestampcheck(T1,true) then

                let aj=XOR(XNj,h(CON(KMS,Tj))) in
                let IDj_1=XOR(XNj,h(CON(KMS,CON(aj,Tj)))) in
                if IDj_1=IDj then
                        let A2=ECC(KMS,A1) in
                        let     Vidj_1=h(CON(IDj,CON(XNj,CON(YNj,CON(A1,CON(A2,h(CON(CON(A2,h(CON(IDj,KMS))),
CON(Tj,T1))))))))) in
                        event BeginMS(IDj);
                        new ai_1:nonce;
                        new bi_1:nonce;
                        let ai=bit_nonce(ai_1) in
                        let bi=bit_nonce(bi_1) in
                        let A3=ECC(bi,P) in
                        let A4=ECC(bi,A1) in
                        let XNjn1=XOR(ai,h(CON(KMS,T2))) in
                        let YNjn1=XOR(IDj,h(CON(KMS,CON(ai,T2)))) in
                        let u=XOR(XNjn1,h(CON(A2,h(CON(CON(CON(IDj,KMS),T2)))))) in
                        let L=XOR(YNjn1,h(CON(T2,CON(A2,h(CON(IDj,KMS)))))) in
                        let KSHi_1=h(CON(A1,CON(A2,CON(A3,CON(A4,CON(IDj,T2)))))) in
                        let D=h(CON(XNjn1,CON(YNjn1,CON(KSHi_1,T2)))) in
                        let KSHi=key_bit(KSHi_1) in
                        out(PC,(u,L,D,A3,T2));
                        event EndMS(IDj).
```

Figure 7: The process of MS.



```
(*--Main process--*)
process
        let KMSn=bit_key(KMS) in
        let Q=ECC(KMSn,P) in
        new aj_1:nonce;
        let aj=bit_nonce(aj_1) in
        new Tj_1:timestamp;
        let Tj=bit_timestamp(Tj_1) in
        let XNj=XOR(aj,h(CON(KMSn,Tj))) in
        let YNj=XOR(IDj,h(CON(KMSn,CON(aj,Tj)))) in
        let MHj=h(CON(IDj,KMSn)) in
        (!SNj(IDj,P,Q,XNj,YNj,MHj)|!mserver(IDj,P,Q,KMSn,Tj))
```

Figure 8: Main process.



```
Verification summary:

Query not attacker(KMS[]) is true.

Query not attacker(KSHj[]) is true.

Query not attacker(KSHi[]) is true.

Query not attacker(IDj[]) is true.

Query event(EndSNj(IDj_4)) ==> event(BeginMS(IDj_4)) is true.

Query inj-event(EndMS(IDj_4)) ==> inj-event(BeginSNj(IDj_4)) is true.

Query inj-event(EndSNj(IDj_4)) ==> inj-event(BeginMS(IDj_4)) is true.
```

Figure 9: Results.

6.2.4. Freshness. If the ensuing requirements are met, INS_P^i can be defined as fresh.

(1) INS_{SN}^i and INS_{MS}^i are in the state Accept

(2) Reveal has not been executed

(3) Corrupt is executed at most once

6.2.5. Semantic Security. The random bit r in *Test* query determines the output of *Test*. Meanwhile, A generates a random r', if $r' = r$, A knows if the output is session key. The advantage of guessing the correct bit is $\text{Adv}_{\mathscr{P}}^{A} = |2\Pr[r = r'] - 1| = |2\Pr[\text{suc}(A)] - 1|$. $\mathscr{P}$ is secure when $\text{Adv}_{\mathscr{P}}^{A} < \eta$, where η is sufficiently small.

CDHP: the CDHP is specified that given P, aP, and bP, computing abP is computationally infeasible in probabilistic polynomial time (PPT). P is the generator point, $a, b \in Z_p$. Subsequently, the advantage of solving CDHP is $\text{Adv}_A^{\text{CDHP}} = \Pr\ [A(P, aP, bP) = abP\colon P \in E(F_p); a, b \in Z_p]$, $\text{Adv}_A^{\text{CDHP}} < \eta$.

Theorem 1. *Suppose the adversary A tends to break the proposed scheme $\mathscr{P}$ in PPT. The queries Execute, Send, and Hash are executed q_E, q_S, and q_H times, respectively. Query Test is allowed to be executed at most once. l_h is the bit-length of the hash operation's the output. $n = 2^{l_t}$, where l_t is the average length of other transcripts. The advantage of breaking $\mathscr{P}$ by A in PPT can be expressed as follows:*

$$\text{Adv}_A^{\mathscr{P}} \leq \frac{(q_S + q_E)^2}{n} + \frac{q_H^2}{2^{l_h}} + 2\text{Adv}_A^{\text{CDHP}} + 2\text{Adv}_A^{\text{PUF}}. \quad (1)$$

Proof. To simulate the attacks on $\mathscr{P}$, we define various games $\text{Game}_i\,(0 < i < 3)$. The event $\text{Success}_A^i\,(0 < i < 3)$ corresponding to Game_i means that A completes his/her goal in Game_i.

Game_0: which simulates the real attack, at the first, the probability of A cracking $\mathscr{P}$ is

$$\text{Adv}_A^{\mathscr{P}} = \left|2\Pr\left[\text{Success}_A^0\right] - 1\right|. \quad (2)$$

Game_1: which simulates that A launches *Execute* and *Test* queries to verify the output according to the transcripts $\{\text{Message1}, \text{Message2}, \text{Message3}, \text{Message4}\}$. Among the transcripts, $\{A_1, \Delta, A_3, T_2\}$ are related to the session key. However, A cannot figure out the relation between them the transcripts and the output of *Test* because of the random numbers. Therefore, we have

$$\Pr\left[\text{Success}_A^1\right] = \Pr\left[\text{Success}_A^0\right]. \quad (3)$$

Game_2: In this game, we simulate A computes the session key K_{SH} through the messages transmitted openly. $K_{SH} = h(A_1, A_2^*, A_3, A_4, id_j^*, T_2)$, which is based on CDHP. The advantage of calculating K_{SH} by A is $\text{Adv}_A^{\text{CDHP}}$. Therefore, we have

$$\Pr\left[\text{Success}_A^2\right] - \Pr\left[\text{Success}_A^1\right] = \text{Adv}_A^{\text{CDHP}}. \quad (4)$$

Table 2: Security properties comparison.

Attacks/Properties	[14]	[25]	[29]	[30]	Ours
Anonymity	Yes	Yes	No	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Forger and impersonation attack	No	Yes	Yes	Yes	Yes
Off-line identity guessing attack	Yes	Yes	No	No	Yes
Sensor node capture attack	Yes	Yes	Yes	Yes	Yes
Smart card loss attack	Yes	Yes	Yes	Yes	Yes
Desynchronization attack	Yes	No	Yes	No	Yes
Stolen-verifier attack	Yes	Yes	Yes	No	Yes
Man-in-middle attack	Yes	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	No	Yes	Yes
Know-key attack	Yes	Yes	No	No	Yes
Untraceability	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	No	No	No	Yes

Game_3: This game simulates A performs $\mathit{Corrupt}(\text{INS}_{SN}^i)$ to acquire the reserved information $\{id_j, x_{Nj}, y_{Nj}, ST_j, Cha_j, T_j\}$ in SN_j and try to calculate $\Delta^* = h({x_{N_j}}^{\text{new}*}, {y_{N_j}}^{\text{new}*}, K_{SH}, T_2)$ to testify the K_{SH}'s correctness, where ${x_{N_j}}^{\text{new}*} = \mu \oplus h(A_2, MH_j, T_2)$, ${y_{N_j}}^{\text{new}*} = \lambda \oplus h(T_2, A_2, MH_j)$, and $MH_j = h(PUF(\text{Cha}_j)) \oplus ST_j$. A has to break PUF to obtain MH_j. The probability of breaking PUF is Adv_A^{PUF}. Therefore, we have

$$\Pr\left[\text{Success}_A^3\right] - \Pr\left[\text{Success}_A^2\right] \leq \text{Adv}_A^{\text{PUF}}. \quad (5)$$

Game_4: which simulates *Execute* and *Send* queries are executed by A to launch the collision attacks. In line with the birthday paradox's definition, the possibility of a hash collision is $q_H^2/2^{l_h+1}$. Meanwhile, the collision probability of other transcripts is $(q_S + q_E)^2/2n$. Hence, we have

$$\Pr\left[\text{Success}_A^4\right] - \Pr\left[\text{Success}_A^3\right] \leq \frac{(q_S + q_E)^2}{2n} + \frac{q_H^2}{2^{l_h+1}}. \quad (6)$$

The random bit $r \in (0, 1)$, the probability of guessing r is 1/2, which is equal to guessing the session key. That is,

$$\Pr\left[\text{Success}_A^4\right] = \frac{1}{2}. \quad (7)$$

Combining (1) with (6), we got

$$\frac{1}{2}\text{Adv}_A^{\mathscr{P}} \leq \frac{(q_S + q_E)^2}{2n} + \frac{q_H^2}{2^{l_h+1}} + \text{Adv}_A^{\text{CDHP}} + \text{Adv}_A^{\text{PUF}}. \quad (8)$$

(8) can be expressed as follows:

$$\text{Adv}_A^{\mathscr{P}} \leq \frac{(q_S + q_E)^2}{n} + \frac{q_H^2}{2^{l_h}} + 2\text{Adv}_A^{\text{CDHP}} + 2\text{Adv}_A^{\text{PUF}}. \quad (9)$$

□

7. Performance Analysis

We study and compare security and performance efficiency between ours with others. According to the comparison of the security attributes which are given in Table 2, we earn better security. In Windows 10 professional 64-bit, Intel(R)

Table 3: The computation cost comparison.

Schemes	Server	SN_j (sensor)	Total
[14]	$5T_{HS}$	$3T_{HS}$	$8T_{HS}\,(0.544ms)$
[25]	$3T_{HS} + 3T_{EA} + 2T_{SE}$	$2T_{HS} + 2T_{EA} + T_{SE}$	$5T_{HS} + 5T_{EA} + 3T_{SE}\,(14.525ms)$
[29]	$6T_{HS}$	$4T_{HS}$	$10T_{HS}\,(0.680ms)$
[30]	$6T_{HS}$	$4T_{HS}$	$10T_{HS}\,(0.680ms)$
Ours	$5T_{HS} + 3T_{EA}$	$13T_{HS} + 3T_{EA}$	$18T_{HS} + 6T_{EA}\,(16.230ms)$

Table 4: The storage cost comparison.

Protocols		Storage cost (bits)	Total (bits)
[14]	Sensor	544	864
	RN	32	
	Server	288	
[25]	Sensor	1536	1952
	RN	0	
	Server	416	
[29]	Sensor	800	1108
	RN	32	
	Server	276	
[30]	Sensor	1056	1664
	RN	32	
	Server	576	
Ours	Sensor	832	928
	RN	32	
	Server	64	

Table 5: The communication cost comparison.

Schemes	[14]	[25]	[29]	[30]	Ours
Communication cost (bits)	4196	2752	3712	3712	3936

Core(TM) i5-4590, we earn $T_{HS} = 0.068$ms (millisecond), $T_{EA} = 2.501$ms, $T_{SE} = 0.56$ms [36], where T_{HS} is hash operation, T_{EA} represents ECC operation, and T_{SE} is symmetric key encryption. As Table 3 revealed, we describe the computational cost comparison between other protocols and the proposed protocol. In [14], the server's and sensor's total computation cost is $5T_{HS} + 3T_{HS} = 8T_{HS}\,(0.544ms)$. Accordingly, the schemes [29, 30] both need $6T_{HS} + 4T_{HS} = 10T_{HS}\,(0.544ms)$, and scheme [25] needs $5T_{HS} + 5T_{EA} + 3T_{SE}\,(14.525ms)$, and ours is $18T_{HS} + 6T_{EA}\,(16.230ms)$. Because our protocol is safer than others and achieves perfect forward secrecy, so ours achieve both high computational efficiency and security.

According to [38], outputs of identity, timestamp, and password are 32 bits, and a random integer, hash function, or block encryption is 256 bits, and a point in the elliptic curve is 160 bits. We calculate the storage overhead of the devices participating in authentication. Storage costs comparison is indicated in Table 4, ours maintain the lowest storage overhead. In addition, messages in login and mutual authentication are transmitted 4 times in our scheme. We calculate our communication costs and others, and ours is equivalent to other schemes from Table 5.

8. Conclusion

We first point out that Alzahrani et al.'s protocol can't defend against stolen-verifier attacks, desynchronization attacks, known-key attacks, and off-line identity guessing attacks and has no perfect forward secrecy. After that, we design a patient monitoring scheme based on ECC for WBAN in IoHT. We use verification tool ProVerif and formal security proof to demonstrate the security of our scheme. Through comparative analysis, our protocol is safer and more efficient to suit the lightweight and secrecy in medical scenarios. In the future, we will research more pragmatic and anonymous authentication protocol for more complex WBAN scenarios.

Data Availability

All data are included in manuscript.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant no. U21A20466) and the National Key R&D Program of China (Grant no. 2017YFB0802000).

References

[1] M. Seyedi, B. Kibret, D. T. Lai, and M. Faulkner, "A survey on intrabody communications for body area network applications," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 8, pp. 2067–2079, 2013.

[2] V. Esteves, A. Antonopoulos, E. Kartsakli, M. Puig-Vidal, P. Miribel-Català, and C. Verikoukis, "Cooperative energy harvesting-adaptive MAC protocol for WBANs," *Sensors*, vol. 15, no. 6, Article ID 12635, 2015.

[3] R. Punj and R. Kumar, "Technological aspects of WBANs for health monitoring: a comprehensive review," *Wireless Networks*, vol. 25, no. 3, pp. 1125–1157, 2019.

[4] B. Narwal and A. K. Mohapatra, "A review on authentication protocols in wireless body area networks (WBAN)," in *Proceedings of the 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 227–232, IEEE, Gurgaon, India, October 2018.

[5] M. Salayma, A. Al-Dubai, I. Romdhani, and Y. Nasser, "Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–38, 2018.

[6] T. Limbasiya and N. Doshi, "An analytical study of biometric based remote user authentication schemes using smart cards," *Computers & Electrical Engineering*, vol. 59, pp. 305–321, 2017.

[7] Q. Liu, K. G. Mkongwa, and C. Zhang, "Performance issues in wireless body area networks for the healthcare application: a survey and future prospects," *SN Applied Sciences*, vol. 3, no. 2, Article ID 155, pp. 1–19, 2021.

[8] H. M. Chen, J. W. Lo, and C. K. Yeh, "An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3907–3915, 2012.

[9] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 37, no. 2, pp. 9911–9918, 2013.

[10] Q. Xie, B. Hu, and N. Dong, "Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems," *PLoS One*, vol. 9, no. 7, Article ID e102747, 2014.

[11] N. Radhakrishnan and A. P. Muniyandi, "Dependable and provable secure two-factor mutual authentication scheme using ECC for IoT-based telecare medical information system," *Journal of Healthcare Engineering*, vol. 2022, Article ID 9273662, 2022.

[12] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *Journal of Medical Systems*, vol. 39, no. 11, pp. 136–138, 2015.

[13] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," *Journal of Medical Systems*, vol. 40, no. 11, Article ID. 231, 2016.

[14] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[15] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Computer Networks*, vol. 140, pp. 138–151, 2018.

[16] M. Soni and D. K. Singh, "LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1067–1084, 2021.

[17] S. U. Jan, S. Ali, I. A. Abbasi, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, Article ID 9954089, 2021.

[18] I. Ullah, S. Zeadally, N. U. Amin, M. Asghar Khan, and H. Khattak, "Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN)," *Microprocessors and Microsystems*, vol. 81, Article ID 103477, 2021.

[19] I. Ullah, M. A. Khan, A. Alkhalifah et al., "A multi-message multi-receiver signcryption scheme with edge computing for secure and reliable wireless internet of medical things communications," *Sustainability*, vol. 13, no. 23, Article ID 13184, 2021.

[20] I. Ullah, A. Alkhalifah, S. U. Rehman, N. Kumar, and M. A. Khan, "An anonymous certificateless signcryption scheme for internet of health things," *IEEE Access*, vol. 9, Article ID 101207, 2021.

[21] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-Health) system," *Journal of Medical Systems*, vol. 45, no. 1, p. 4 2021.

[22] M. A. Khan, S. U. Rehman, M. I. Uddin et al., "An online-offline certificateless signature scheme for internet of health things," *Journal of Healthcare Engineering*, vol. 2020, Article ID 6654063, 10 pages, 2020.

[23] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 40, no. 6, p. 134 2016.

[24] R. Chen and D. Peng, "Analysis and improvement of a mutual authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 43, no. 2, pp. 19–10, 2019.

[25] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K. K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, vol. 61, pp. 238–249, 2017.

[26] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, 2020.

[27] S. Kalra and S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *Journal of Information Security and Applications*, vol. 20, pp. 37–46, 2015.

[28] C. Chunka, S. Banerjee, and R. S. Goswami, "An efficient user authentication and session key agreement in wireless sensor network using smart card," *Wireless Personal Communications*, vol. 117, no. 2, pp. 1361–1385, 2021.

[29] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 14, Article ID e5295, 2019.

[30] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Communications*, vol. 117, no. 1, pp. 47–69, 2021.

[31] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[32] B. Hu, W. Tang, and Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments," *Neurocomputing*, vol. 500, pp. 741–749, 2022.

[33] T. Jabeen, H. Ashraf, and A. Ullah, "A survey on healthcare data security in wireless body area networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9841–9854, 2021.

[34] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[35] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: a tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[36] M. Potkonjak and V. Goudar, "Public physical unclonable functions," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1142–1156, 2014.

[37] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, *ProVerif 2.00: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial*, pp. 05–16, 2018.

[38] Q. Xie, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1382–1392, 2017.

Hindawi
Journal of Healthcare Engineering
Volume 2022, Article ID 7745132, 14 pages
https://doi.org/10.1155/2022/7745132

Research Article

Multi-Chaos-Based Lightweight Image Encryption-Compression for Secure Occupancy Monitoring

Yazeed Yasin Ghadi,[1] Suliman A. Alsuhibany,[2] Jawad Ahmad,[3] Harish Kumar,[4] Wadii Boulila,[5,6] Mohammed Alsaedi,[7] Khyber Khan,[8] and Shahzad A. Bhatti[9]

[1] *Department of Computer Science and Software Engineering, Al Ain University, Abu Dhabi 15551, UAE*
[2] *Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia*
[3] *School of Computing, Edinburgh Napier University, Edinburgh, UK*
[4] *Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia*
[5] *Robotics and Internet of Things Lab, Prince Sultan University, Riyadh, Saudi Arabia*
[6] *RIADI Laboratory, University of Manouba, Manouba, Tunisia*
[7] *College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia*
[8] *Department of Computer Science, Khurasan University, Jalalabad, Afghanistan*
[9] *Department of Electrical and Electronic Engineering, University of Strathclyde, Glasgow, UK*

Correspondence should be addressed to Khyber Khan; khyber.khan.khurasan@gmail.com

Received 12 March 2022; Revised 2 April 2022; Accepted 7 April 2022; Published 8 November 2022

Academic Editor: Muhammad Asghar Khan

With the advancement of camera and wireless technologies, surveillance camera-based occupancy has received ample attention from the research community. However, camera-based occupancy monitoring and wireless channels, especially Wi-Fi hotspot, pose serious privacy concerns and cybersecurity threats. Eavesdroppers can easily access confidential multimedia information and the privacy of individuals can be compromised. As a solution, novel encryption techniques for the multimedia data concealing have been proposed by the cryptographers. Due to the bandwidth limitations and computational complexity, traditional encryption methods are not applicable to multimedia data. In traditional encryption methods such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), once multimedia data are compressed during encryption, correct decryption is a challenging task. In order to utilize the available bandwidth in an efficient way, a novel secure video occupancy monitoring method in conjunction with encryption-compression has been developed and reported in this paper. The interesting properties of Chebyshev map, intertwining map, logistic map, and orthogonal matrix are exploited during block permutation, substitution, and diffusion processes, respectively. Real-time simulation and performance results of the proposed system show that the proposed scheme is highly sensitive to the initial seed parameters. In comparison to other traditional schemes, the proposed encryption system is secure, efficient, and robust for data encryption. Security parameters such as correlation coefficient, entropy, contrast, energy, and higher key space prove the robustness and efficiency of the proposed solution.

1. Introduction

A fully automatic human occupancy information system has various commercial applications [1], for example, passenger counting, identifying hourly office patterns, and counting shopping center footfall. Researchers have proposed various occupancy measurement solutions through various sensors over the last two decades [1]. These sensors include camera, passive infrared (IR), ultrasonic, CO_2, Wi-Fi, and radio frequency (RF) identifiers [2]. However, it is reported that camera-based human occupancy techniques are more accurate when compared to other sensor-based methods. The biggest issue with the camera-based occupancy is monitoring occupancy with privacy preservation [2, 3]. In such scenarios, encryption can play a vital role and can hide the information and identity of individuals during the occupancy process [3]. In video encryption, identity of individuals is concealed and only an authorized person who has correct key information can decrypt the original video contents [4].

Images and videos can be encrypted using traditional schemes such AES and DES; however, these schemes are not designed for multimedia data encryption [5–7]. Conventional encryption schemes have some issues such as higher computational complexity as images contain large amount of data and strong correlation among pixels. As a result, traditional encryption schemes fail to satisfy real-time implementation constraints and thus have limited applications in the real-time multimedia applications [8]. To overcome the aforementioned issues, chaotic maps can provide highly secure encryption due to complex dynamics and ergodicity.

Mathews introduced the concept of chaos-based encryption algorithms [9], and since then many algorithms using chaos theory have been proposed [10]. For example, a novel image encryption scheme based on Henon and Ikeda chaotic maps and a lattice model based on Arnold coupled logistic map (ACLM) have been proposed in [11, 12]. In the lattice model, the coupling coefficients are generated from the logistic map that is further employed in diffusion and permutation processes. Moreover, ACLM is employed in key generation and an efficient scheme is presented. Saiyma et al. proposed a novel encryption algorithm using Rubik's cube puzzle and logistic chaotic map for pixel permutation and diffusion [13]. Another encryption scheme that utilizes Rubik's cube puzzle for the permutation of bits and XOR operation for diffusion was proposed in [14].

A key-based block ciphering method was presented in [15] where pixel bytes are encrypted and shuffled using variable block sizes that enhance the diffusion property. Zhao and Ren [16] employed infinite-dimensional hyperchaotic multi-attractor (HCMA) Chen system that was generated by a linear time-delay feedback control for the encryption of digital images. In [17], piecewise linear chaotic map (PLCM) and S-Box transformation are applied on original plaintext image. Furthermore, an XOR operation is applied to the diffused image pixels. Elements for XOR operations were based on mixing of chaotic logistic random sequence. A hybrid chaos-based random stream and blockwise encryption algorithm with a key stretching method for the enhancement of security was presented in [18]. Chai et al. [19] proposed an image compression and encryption scheme by combining a parameter-varying chaotic system, elementary cellular automata (ECA), and block compressive sensing (BCS). Musanna et al. proposed a secure image encryption using multi-chaotic maps and multi-resolution singular value decomposition (MR-SVD) for secure image encryption [20].

In [21], fractional Fourier transform (FRFT), DNA sequencing, and chaos theory have been used for image security. However, there are several issues in DNA-based image encryption [22]. These issues were higher computational complexity and inappropriate implementation. In order to address the drawbacks of DNA-coding-based encryption algorithms, a new technique was introduced in [22] which is based on the integer wavelet transform (IWT) and global bit scrambling (GBS) for image encryption. Previously, video and image encryption schemes have been proposed, but they are either insecure or impractical.

2. Preliminaries

2.1. Chaotic Maps. Any mathematical function that exhibits chaotic behavior is known as chaotic map. A close association between chaos and cryptography has been widely reported in literature since many decades. This close relationship is due to high sensitivity of initial conditions, deterministic dynamics, and attack complexity of chaotic map. Logistic map shown in equation (1) is an example of one-dimensional (1D) chaotic map [23]:

$$Z_{n+1} = \mu Z_n \left(1 - Z_n\right), \tag{1}$$

where the initial parameters are

$$\begin{aligned} Z_0 &\in (0, 1), \\ \mu &\in (0, 4). \end{aligned} \tag{2}$$

The bifurcation diagram of logistic map is shown in Figure 1. It is clear from Figure 1 that the logistic map has chaotic behavior for the range $3.57 \leq \mu \leq 4$. Any variation of μ within this range results in a random output of the logistic map. Range of μ is low and hence an intruder can apply exhaustive key search attack.

The key processes of an image encryption technique are confusion and diffusion. In our proposed scheme, Chebyshev and intertwining chaotic maps are employed in confusion and diffusion processes. Mathematically, Chebyshev map can be defined as [24, 25]

$$T_k(A) = \cos\left(k \times \arccos(A)\right), \tag{3}$$

where k is an integer and $A \in [-1, 1]$. It is proposed that $k = 4$ for less computation requirements [25].

The intertwining map can be written as [26]

$$\begin{aligned} X_{n+1} &= \left(\lambda \times A_1 \times Y_n \times \left(1 - X_n\right) + Z_n\right) \bmod (1), \\ Y_{n+1} &= \left(\frac{\lambda \times A_2 \times Y_n + Z_n}{1 + \left(X_{n+1}\right)^2}\right) \bmod (1), \\ Z_{n+1} &= \lambda \times \left(X_{n+1} + Y_{n+1} + A_3\right) \times \sin\left(Z_n\right) \bmod (1), \end{aligned} \tag{4}$$

where X_n, Y_n, and $Z_n \in (0, 1)$, $0 \leq \mu \leq 3.999$, $|A_1| > 33.5$, $|A_2| > 37.9$, $|A_3| > 35.7$. Key space of intertwining logistic map is $10^{60} \approx 2^{200}$ which reduces the possibility of brute force attack.

2.2. Substitution Box. In symmetric key cryptography, substitution is a nonlinear bijective function. Generally, m bits are given as an input to substitution box (S-Box), and as a result, n bit output is produced [27, 28]. In case of digital images, the bijective function $F\colon I \longrightarrow S$ maps each image

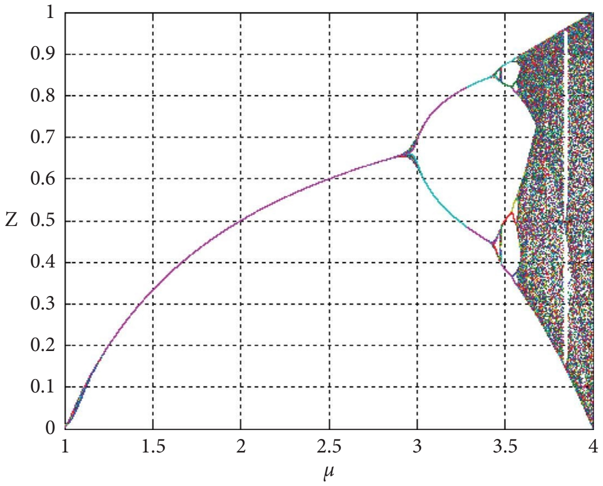


Figure 1: Bifurcation diagram (μ spacing is 0.0005).

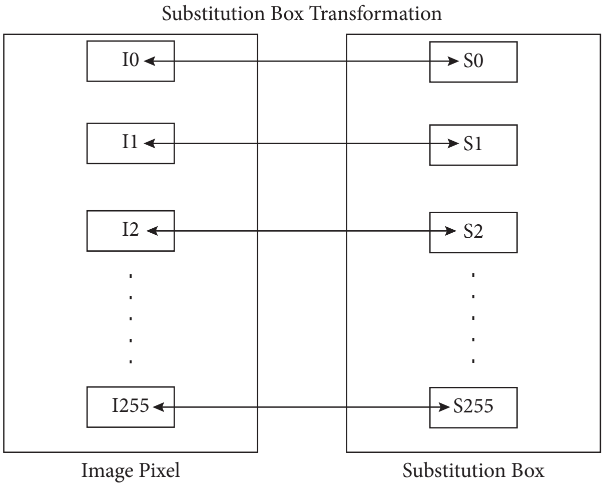


Figure 2: Bijective mapping of substitution box.

pixel I to a unique value S as shown in Figure 2. In many traditional algorithms such as AES and DES, S-Box is the only nonlinear part of ciphertext. In our previous research, it has been highlighted that substitution-only image encryption scheme is highly vulnerable to various types of attacks. Thus, the use of a single S-Box in image encryption algorithms is not a good choice due to weaker security. Instead of a single fixed S-Box, we have used three S-Boxes known as AES S-Box [29], Khan's S-Box [30], and Tayseer's S-Box [31], respectively. Due to higher nonlinearity and good resistance against different attacks, we have selected these S-Boxes in our proposed scheme. These S-Boxes are outlined in Tables 1–3. In the proposed scheme, S-Box is randomly selected using logistic map. The selection of S-Box is based on logistic map which is further explained in later part of the paper.

2.3. Discrete Cosine Transform. Discrete cosine transform (DCT) is a widely used transform for image compression. The DCT and inverse DCT of a plaintext image P is shown in equations (5) and (6), respectively. The DCT $\Delta(u,v)$ of a plaintext image P is written as [32]

$$\Delta(u,v)=\frac{2}{\sqrt{A\times B}}\Gamma(u)\Gamma(v)\sum_{x=0}^{A-1}\sum_{y=0}^{B-1}P(x,y)\cos\left[\frac{(2y+1)u\pi}{2A}\right]\times\cos\left[\frac{(2x+1)v\pi}{2B}\right], \tag{5}$$

$$P(x,y)=\frac{2}{\sqrt{A\times B}}\Gamma(u)\Gamma(v)\sum_{x=0}^{A-1}\sum_{y=0}^{B-1}\Delta(u,v)\cos\left[\frac{(2y+1)u\pi}{2A}\right]\times\cos\left[\frac{(2x+1)v\pi}{2B}\right], \tag{6}$$

where $n\times n$ is the size of image and $\Gamma(u)$ and $\Gamma(v)$ can be written as

$$\Gamma(u)=\Gamma(v)=\begin{cases}\frac{1}{\sqrt{2}}, & \text{for}\ \frac{u}{v}=0,\\ 1, & \text{otherwise.}\end{cases} \tag{7}$$

An encryption scheme is divided into two types: (i) full encryption and (ii) partial encryption. In full encryption, the complete image is encrypted, while in partial encryption, only a part of the image is encrypted. Partial encryption effectively reduces computational complexity. When an image is converted to frequency domain such as applying discrete cosine transform (DCT), less attention is given to higher frequency components.

3. The Proposed Real-Time Secure Occupancy Monitoring System

The proposed scheme uses multi-chaos for the encryption of real-time frames obtained from an overhead 2.0 megapixels Logitech camera installed at a height of 1.7 m above the floor in T10 office at Glasgow Caledonian University, United Kingdom. Figure 3 shows real-time frames with one, two, and three occupants, respectively. In order to protect these frames from eavesdropper, a novel lightweight secure occupancy monitoring system is proposed. Flowchart of the proposed encryption-compression system is depicted in Figure 4. It can be seen from Figure 4 that after discrete cosine transformation (DCT), a block starting from direct coefficient (DCT-DC) is selected and then encrypted through confusion (scrambling) and diffusion (substitution) processes. A part of DCT values is selected

Table 1: AES S-Box [29].

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	22	, 121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Table 2: Khan's S-Box [30].

129	148	14	206	208	63	95	219	86	242	69	254	152	215	53	104
47	138	93	200	161	75	230	110	133	103	24	251	106	159	38	167
181	179	31	218	74	155	153	43	249	0	57	52	162	144	243	235
61	108	164	82	117	213	130	99	228	49	39	12	199	189	78	13
116	175	58	180	123	3	194	232	105	22	65	160	5	84	54	102
56	196	66	182	171	212	131	115	183	67	90	64	15	191	60	178
216	204	248	70	73	118	100	146	7	198	207	137	141	94	92	165
202	221	197	127	23	128	85	252	168	233	68	201	174	76	81	124
220	173	170	225	16	62	25	107	145	46	20	41	122	17	192	187
45	244	247	227	156	157	101	214	71	79	222	226	112	139	30	72
210	172	37	253	239	89	119	35	88	147	97	83	154	33	149	11
4	36	50	176	21	224	120	158	184	51	87	9	114	246	231	217
241	42	240	211	229	250	236	125	136	48	190	237	8	98	27	29
203	193	1	205	188	91	245	143	6	177	96	166	80	142	185	40
140	111	113	55	28	195	26	234	209	135	32	186	134	151	126	132
169	223	10	163	34	19	77	150	44	255	2	121	109	59	238	18

Table 3: Tayseer's S-Box [31].

9	47	204	29	78	208	201	73	23	174	118	109	77	176	227	154
232	42	173	97	179	8	192	161	248	61	60	107	66	49	131	79
146	254	22	25	101	224	30	202	18	134	251	19	213	215	40	102
135	178	184	167	36	105	113	48	3	114	199	164	76	217	89	236
55	156	126	159	75	142	147	58	218	219	7	38	168	45	175	234
214	186	41	5	133	221	228	63	225	1	144	235	162	50	207	163
103	81	108	88	209	165	31	127	11	80	194	187	10	198	120	153
132	98	110	148	0	100	46	250	253	57	33	32	151	14	28	150
52	12	242	252	149	106	13	95	26	96	237	177	205	243	82	85
2	239	190	140	43	203	181	6	139	238	116	64	83	44	56	245
125	70	15	51	183	27	196	39	230	121	143	35	223	128	4	21
229	244	90	111	20	62	93	145	137	67	141	185	206	233	182	59
226	249	119	160	166	200	197	240	17	117	72	37	180	171	91	74
189	222	123	122	112	169	155	193	71	212	124	24	247	129	210	170
104	255	130	152	241	65	68	99	195	136	87	53	92	231	86	34
191	84	211	188	16	138	216	172	220	69	54	246	157	115	158	94

and then encrypted. Let the output after DCT be η and the selected block be $\lambda_{M\times N}$; then, it is multiplied with an orthogonal matrix ψ and the result is stored in Φ. The values obtained in Φ are forwarded to the confusion and diffusion stage. Due to the lightweight nature of Chebyshev and intertwining maps, they are deployed in the confusion and

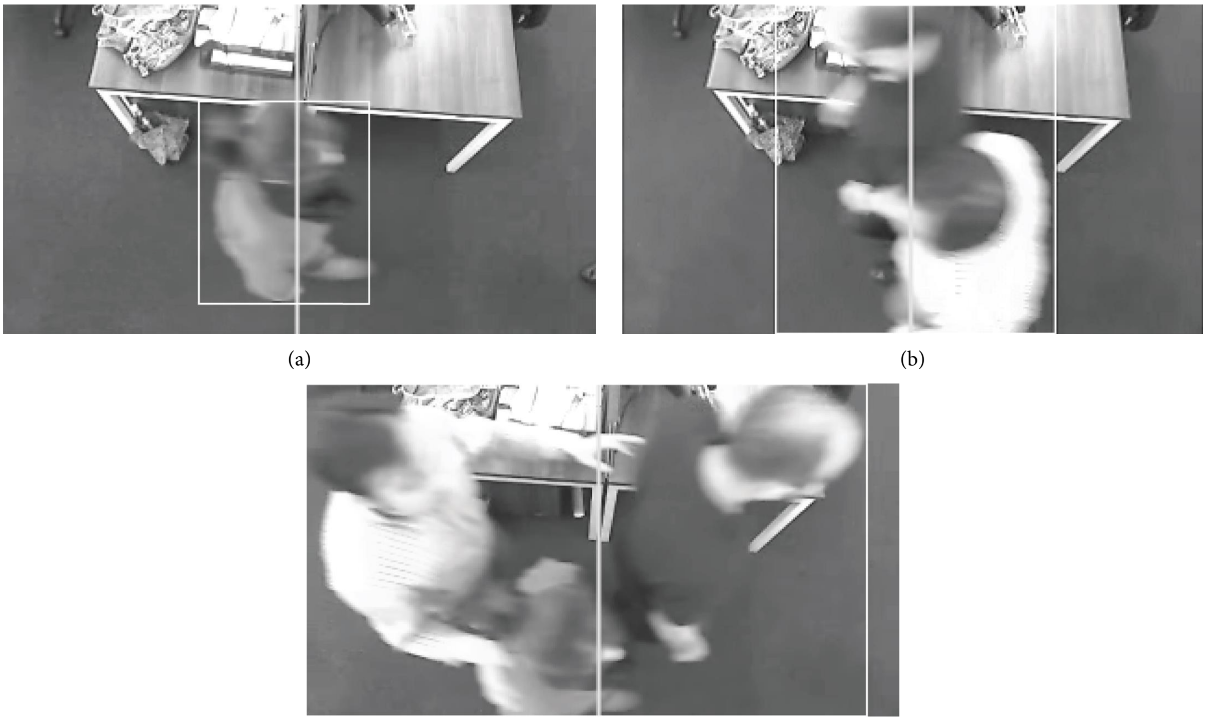


Figure 3: Real-time video frames with different number of occupants. (a) One person. (b) Two persons. (c) Three persons.

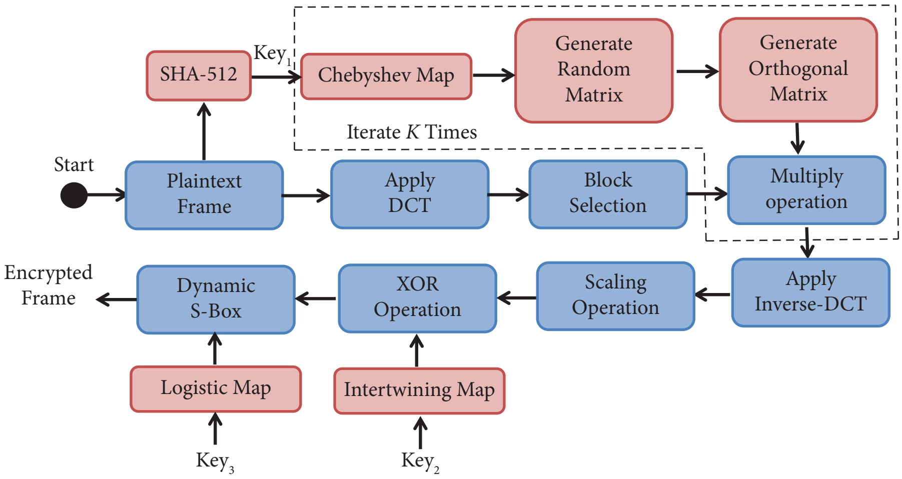


Figure 4: Flowchart of the proposed encryption-compression scheme.

diffusion process of encryption. After the encryption-compression phase, encrypted pixels are transmitted over the channel.

Let the size of a plaintext image P be $A \times B$. In this work, k represents iteration number and ranges from $k = 1$ to N, where N is the total number of iteration. When $k = 1$, the secure hash algorithm (SHA-512) is applied to the plaintext image P for the generation of initial keys for the Chebyshev map. Detailed steps of the proposed scheme are outlined as follows:

(1) Apply DCT on plaintext image P to get η.

(2) Select DCT coefficients from η, staring from the DCT-DC coefficient to get λ. The dimensions of the selected coefficients matrix can be same or different as compared to the original image. Let the size of λ be $M \times N$.

(3) Iterate a $M \times N$ Chebyshev map to get random matrix Λ.

(4) Apply the Gram–Schmidt algorithm to the random matrix Λ to get an orthogonal matrix Φ.

(5) Multiply λ and Φ and get a new matrix ϕ. Repeat steps from 3 to 5 for N times. In each iteration,

values of initial conditions are slightly changed and σ is added in original initial value, where $\sigma = 0.001$.

(6) Apply inverse DCT and map the values to the 0–255 range to get ω.

(7) Iterate a intertwining map $M \times N$ times to get a random row vector f.

(8) Multiply the row vector f with 10^{14} and apply mod operation using the following equation:

$$\alpha = \left|\left(10^{14} \times f\right)\right| \bmod (256), \tag{8}$$

where $|\cdot|$ is the absolute value. Reshape row matrix α into $M \times N$ and get β.

(9) Perform XOR operation between ω and β to get a new matrix ζ.

(10) Randomly select a S-Box using logistic map and apply S-Box on ζ to get the final ciphertext C. The output of logistic map is multiplied with a factor 10^{14} to get ψ and apply Mod 3 operator to get Ψ. If the value in Ψ is 0, 1, and 2, then AES S-Box, Khan's S-Box, and Tayseer's S-Box are selected, respectively.

Decryption is the reverse process of encryption and all steps can be applied in the reverse process to get the original plaintext image.

4. Security Analyses

Results of the proposed encryption scheme are shown in Figures 5–8. In the first test (Figure 5), the size of DCT block is the same as plaintext image size, and hence both plaintext and ciphertext image frames have same sizes. From Figure 5, one can see that the proposed scheme hides the original contents of the frame and hence the number of occupant information is also concealed. The decryption results are shown in Figure 6. In the second test, the size of DCT block is selected as $M \times N/2 \times 2$, and as a result, the size of encrypted image is 4 times less than the plaintext size. The encryption and decryption results are shown in Figures 7 and 8, respectively. In Figure 7, it can be seen that size of ciphertext is 4 times smaller than the plaintext image and still correct decryption (see Figure 8) is possible. This type of compression is not possible in traditional encryption. From the visual inspection in Figures 5 and 7, it is evident that the proposed scheme encrypts the original information; however, the security of an encryption algorithm should be statistically proved.

4.1. Correlation Coefficient. Degree of similarity between two variables can be measured via correlation coefficient metric. In image processing, correlation is the degree of similarity between two images. One can also check the correlation between two adjacent pixels (horizontal, vertical, and diagonal) through selection of random pairs. The lower the value of correlation coefficient, the higher the security of image encryption scheme.

The correlation coefficient can be computed using the following mathematical formula:

$$r = \frac{\text{Covariance}(x, y)}{S_x \times S_y}, \tag{9}$$

where S_x and S_y are standard deviation at pixel positions x and y, respectively. Covariance is written as

$$\begin{aligned} \operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ S_x &= \sqrt{\text{Variance}(x)}, \\ S_y &= \sqrt{\text{Variance}(y)}. \end{aligned} \tag{10}$$

In order to check the strength of the proposed encryption scheme, we evaluated correlation coefficients in horizontal, vertical, and diagonal directions, for Figures 3 and 5, respectively. Correlation plots in diagonal direction are shown in Figure 9. From these plots, it can be seen that original images have correlated distribution in diagonal direction but encrypted images have uncorrelated distribution for all test images. Similar results were obtained for horizontal and diagonal directions. The correlation values between −1 and 1 are shown in Table 4. From the table, it is clear that when compared to the plaintext image, encrypted image has low correlation values.

4.2. Entropy. The term entropy refers to statistical measure of randomness or uncertainty. In image processing, entropy calculates the distribution of gray values. For a gray scale image with 256 gray levels, ideally the information entropy must be 8 bits for a complete random image. Mathematically, entropy is defined as

$$H(m) = \sum_{i=0}^{L-1} p(m_i)\log_2 \frac{1}{p(m_i,)}, \tag{11}$$

where $L = 2^g$. The value of g is 8 for gray images. The entropy values of plaintext and ciphertext images are shown in Table 5. When an image is encrypted using the proposed scheme, the entropy value is close to 8.

4.3. Encryption Quality. One of the important aspects in image security evaluation is to check the quality of encryption. One can check the quality of encryption via visual inspection; however, the security of encryption scheme should be mathematically proved. To check the quality of encryption, a wide range of attributes must be considered during the designing stage of an encryption scheme. Most of the attributes are outlined in our previous work [33–36]. An image encryption is considered good if it hides a wide range of those attributes. Out of many attributes, deviation in pixel values between the original and encrypted images is a robust parameter to evaluate the quality of encryption. Encryption quality is better if deviation between plaintext and ciphertext is maximum and irregular. Three different parameters can be considered to check the deviation of pixels, i.e., maximum

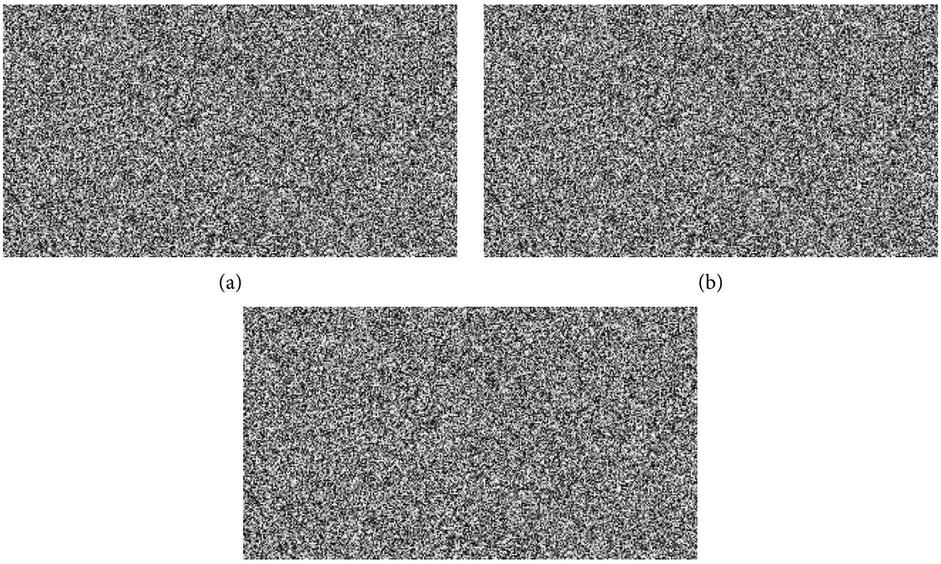

(a) (b) (c)

Figure 5: Real-time encryption with DCT size same as plaintext size. (a) One person. (b) Two persons. (c) Three persons.

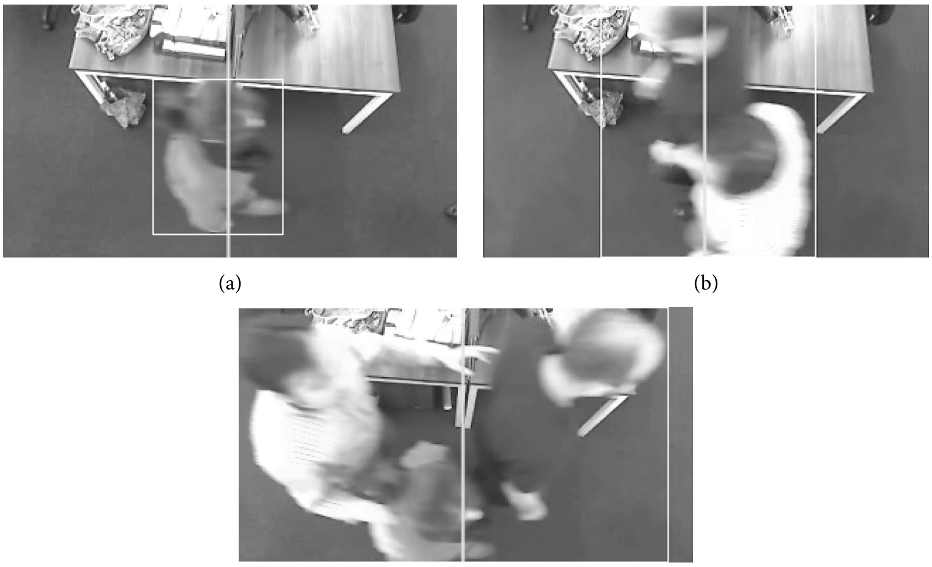

(a) (b) (c)

Figure 6: Decryption results of Figure 5. (a) One person. (b) Two persons. (c) Three persons.

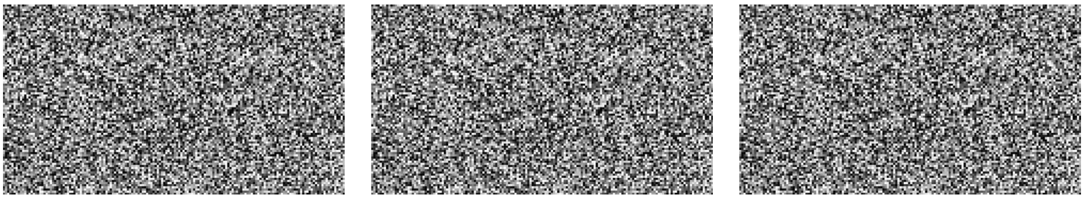

(a) (b) (c)

Figure 7: Encryption results with DCT size $M \times N/2 \times 2$. (a) One person. (b) Two persons. (c) Three persons.

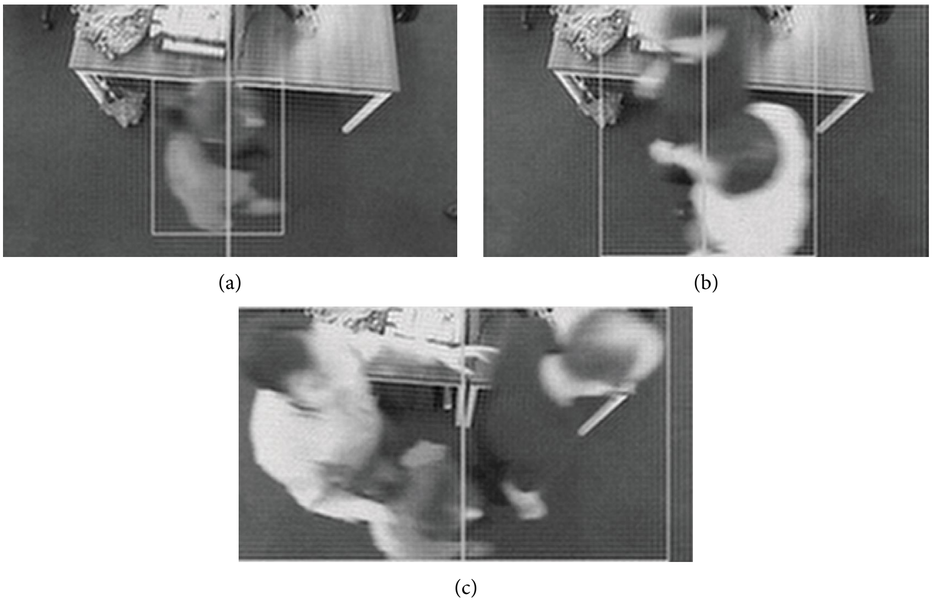


Figure 8: Decryption results with DCT size $M \times N/2 \times 2$. (a) One person. (b) Two persons. (c) Three persons.

deviation (MD), irregular deviation (ID), and deviation from uniform histogram (DUH).

4.3.1. Maximum Deviation (MD). MD measures the deviation between original and encrypted images. A higher value of maximum deviation indicates higher deviation. Maximum deviation is calculated in three steps:

(1) Calculate histograms for the original plaintext image P and the encrypted image C.

(2) Compute the histogram difference (HD) where HD is the absolute deviation (difference) between the histograms calculated in Step 1.

(3) Finally, compute MD as given below:

$$\mathrm{MD} = \frac{\mathrm{HD}_0 + \mathrm{HD}_{N-1}}{2} + \sum_{i=1}^{N-2} \mathrm{HD}_i, \tag{12}$$

where HD_i is the difference histogram at index i.

4.3.2. Irregular Deviation (ID). ID reveals how much of the deviation induced by the encryption algorithm on the ciphertext image is irregular. Lower value of irregular deviation indicates good encryption quality. Steps involved in the calculation of irregular deviation are given as follows:

(1) Compute the average sum of histogram values.

(2) Take the absolute difference (AD) between the average sum of histogram (Avg) and amplitude of histogram at index $i\,(h_i)$. Mathematically, it is written as

$$\mathrm{AD} = \mathrm{Avg} - h_i. \tag{13}$$

(3) Finally compute ID as

$$\mathrm{ID} = \sum_{i=0}^{N-1} \mathrm{AD}. \tag{14}$$

4.3.3. Deviation from Uniform Histogram (DUH). A uniform histogram of an encrypted image is desired for good encryption quality. Less deviation from uniform histogram shows better quality of encryption. For gray scale images, ideal histogram (ID) and the deviation from uniform histogram (DUH) are measured as [37]

$$\mathrm{IH}_i = \begin{cases} \dfrac{A \times B}{256}, & 0 \le C_i \le 255, \\ 0, & \text{elsewhere}. \end{cases} \tag{15}$$

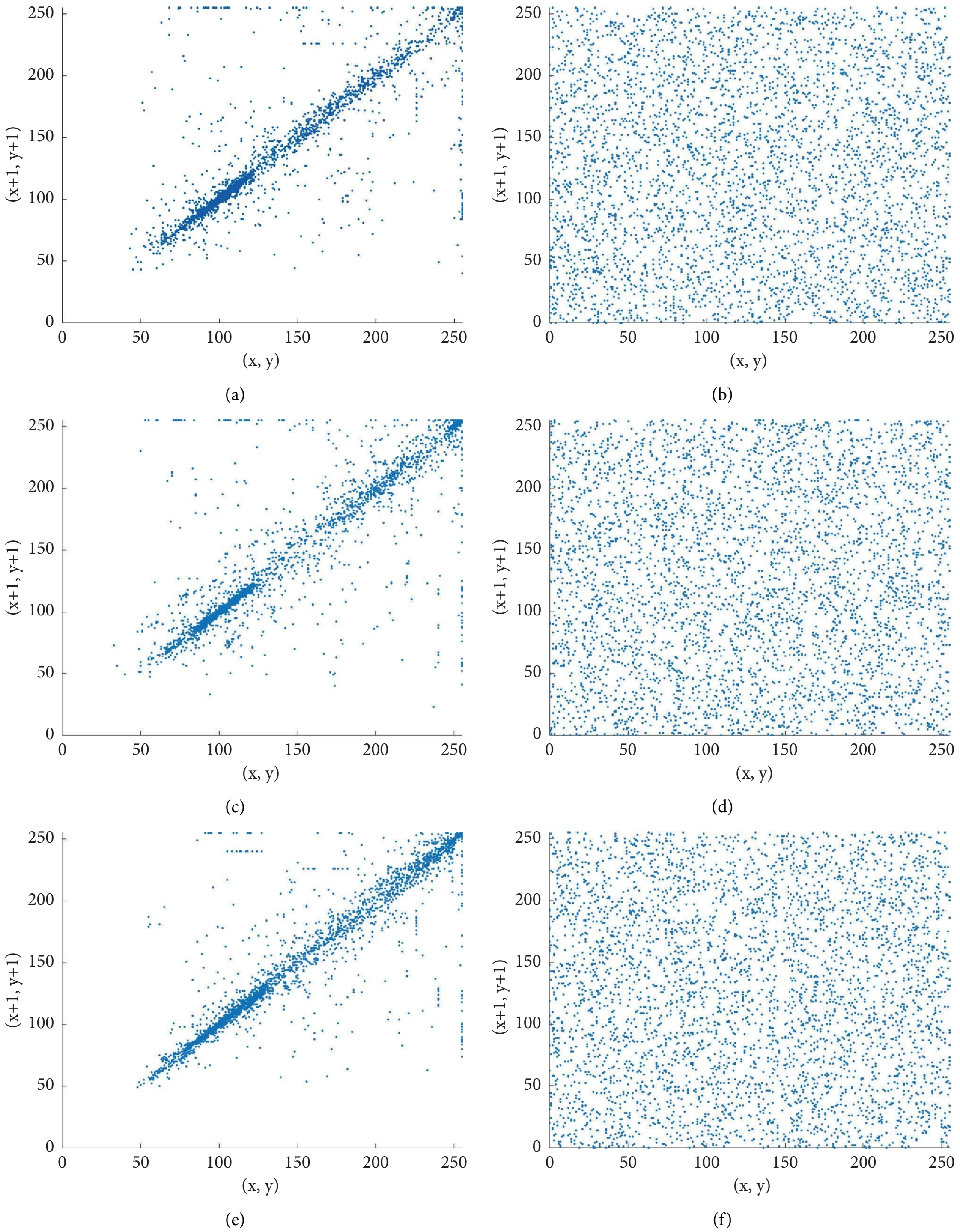
Using the above concept, Abd El-Samie et al. proposed a new metric [37] (DUH) for measuring the quality of encrypted images. DUH is calculated as [37]

$$\mathrm{DUH} = \frac{\sum_{i=0}^{255} \left| \mathrm{IH}_i - H_C \right|}{A \times B}, \tag{16}$$

where H_C is the actual histogram value of ciphertext image.

The MD, ID, and DUH are shown in Table 6. All values confirm the higher security of the proposed scheme.

4.4. Energy. Gray-level co-occurrence matrix (GLCM) is a statistical analysis of texture measurement that reflects the spatial property of image pixels. A squared sum of GLCM elements is energy. For plaintext images, some pixels have large values in gray-level co-occurrence matrix due to which the energy values are high but for ciphertext images, the values of energy are smaller because of the distributed energy values. The energy analysis can be done using the following equation.



(a)

(b)

(c)

(d)

(e)

(f)

Figure 9: Plot of correlation coefficients in diagonal direction. (a) Original image (Figure 3(a) correlation plot). (b) Encrypted image (Figure 5(a) correlation plot). (c) Original image (Figure 3(b) correlation plot). (d) Encrypted image (Figure 5(b) correlation plot). (e) Original image (Figure 3(c) correlation plot). (f) Encrypted image (Figure 5(c) correlation plot).

$$E = \sum_{i,j} p(i, j)^2, \tag{17}$$

where $p(i, j)$ is the position of pixels in gray-level co-occurrence matrix. For a constant image, energy value is equal to 1. Lower values indicates higher randomness in image pixels. The energy values of the plaintext images and the corresponding ciphertext images are shown in Table 7 which shows that the energy values of the ciphertext images are very small.

4.5. Contrast. Contrast measures the variation in GLCM. With the help of contrast, a viewer can differentiate

Table 4: Correlation coefficient values for horizontal, diagonal, and vertical directions.

Images	Plaintext image			Encrypted image		
	H-D	D-D	V-D	H-D	D-D	V-D
1	0.9049	0.8347	0.9068	0.0108	−0.0134	0.0085
2	0.9081	0.8631	0.9480	0.0190	0.0253	0.0179
3	0.9580	0.9020	0.9467	0.0212	−0.0268	−0.0108

Table 5: Entropy analysis.

Images	Original image	Encrypted image
1	6.6776	7.9960
2	6.8434	7.9962
3	7.1017	7.9966

Table 6: Encryption quality analyses.

Images	MD	ID	DUH
1	5.8515×10^4	40046	0.0253
2	5.9088×10^4	37658	0.0292
3	4.8168×10^4	36622	0.0280

Table 7: Energy analysis.

Images	Original image	Ciphertext image
1	0.2631	0.0156
2	0.2487	0.0156
3	0.2159	0.0156

Table 8: Contrast analysis.

Images	Original image	Ciphertext image
1	0.4274	10.4808
2	0.6047	10.5440
3	0.3435	10.6562

Table 9: Homogeneity analysis.

Images	Original image	Ciphertext image
1	0.9351	0.3892
2	0.9210	0.3894
3	0.9394	0.3875

Table 10: Structural content and average difference analysis.

Images	SC	AD
1	0.8228	−2.6914
2	1.0104	9.5119
3	1.1119	16.8750

Table 11: Encryption/decryption time analysis with different DCT sizes.

DCT size	Encryption time (sec)
$M\times N/2\times2$	0.0212
$M\times N/4\times4$	0.0117
$M\times N/8\times8$	0.0095
$M\times N/16\times16$	0.0092

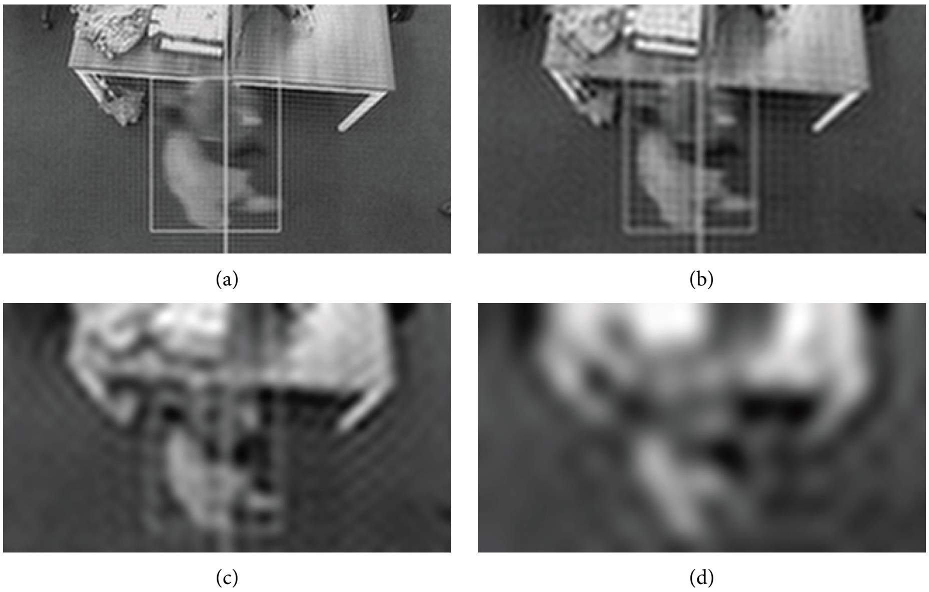


Figure 10: Effect of different DCT sizes. (a) DCT size $M \times N/2 \times 2$. (b) DCT size $M \times N/4 \times 4$. (c) DCT size $M \times N/8 \times 8$. (d) DCT size $M \times N/16 \times 16$.

between the different objects of an image. A higher value of contrast is required for an encrypted image. For a constant image, the value of contrast is 0. Contrast of an image is measured as

$$C = \sum_{i,j} |i - j|^2 \times p(i, j), \tag{18}$$

where $p(i, j)$ indicates the number of GLCM. The values of contrast for plaintext images and ciphertext images are tabulated in Table 8 which clearly indicates that the contrast values of the ciphertext images are very large as compared to the contrast values of plaintext images.

4.6. Homogeneity. Another parameter that can be deduced from GLCM is homogeneity. Homogeneity is the closeness of element distribution in the GLCM. For an efficient image encryption algorithm, the homogeneity values should be low. For determination of homogeneity, the equation used is

$$\text{HOM} = \sum_{i,j} \frac{p(i, j)}{1 + |i - j|}, \tag{19}$$

where $p(i, j)$ represents the gray-level co-occurrence matrices in GLCM. The homogeneity values of the test images are shown in Table 9. It is clear from Table 9 that the proposed scheme provides higher security for plaintext images as the values of homogeneity are lower for encrypted images.

4.7. Structural Content and Average Difference. To determine the similarity between plaintext image and its corresponding ciphertext image, the structural content test can also be applied. It indicates their level of similarities. When the two images are totally different from one another, the value of structural content is 0 and a value of 1 means identical images. In case of image encryption, the value of structural content should be near 0. Mathematical expression for structural content is

$$\text{SC} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(O_{(i,j)}\right)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(E_{(i,j)}\right)^2}, \tag{20}$$

where $O_{(i,j)}$ is the original image and $E_{(i,j)}$ is the encrypted image. Values of structural content can be observed from Table 10.

4.8. Key Space Analysis. The strength of an encryption technique is hidden in secret key parameter. Therefore, key is the most critical feature of a cryptosystem. Smaller key space may lead to expose the full key or a part of key. In digital image encryption, larger key space indicates resistance against the brute force attack. In this work, we have used three chaotic maps and total initial conditions are 8, and as a result, key space (KS) is written as

$$\begin{aligned} \text{KS} &= 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \\ &= 10^{120} \approx 2^{400}. \end{aligned} \tag{21}$$

From the above KS analysis, one can see that the proposed scheme provides sufficient larger key space and hence it is resistant to a number of exhaustive key search attacks and brute force attacks.

4.9. Computational Complexity Analysis. The proposed scheme is tested and implemented in MATLAB R2019b on a PC with 2.70 GHz CPU and 8 GB RAM. When the size of selected DCT block and plaintext image is same, encryption

Figure 11: Cameraman image.

Table 12: Security comparison.

Security parameter	Reference [39]	Reference [40]	Reference [38]	Proposed
Correlation coefficient	0.1156	−0.0012	0.4952	0.0010
Entropy	7.7015	7.9884	7.2825	7.9969
Maximum deviation	6.8×10^4	5.6×10^4	8.1×10^4	6.2×10^4
Irregular deviation	3.9×10^4	3.6×10^4	6.0×10^4	3.7×10^4
Deviation from UH	0.2629	0.0407	0.4690	0.0273
Energy	0.0174	0.0159	0.0594	0.0156
Contrast	8.9473	9.9797	1.6256	10.5064
Homogeneity	0.4587	0.3973	0.6217	0.3890

takes approximately 0.063 seconds. Decryption is the reverse process of encryption and it also takes 0.063 seconds. It is clear from Table 11 that when size of DCT block reduces, encryption time also reduces. In other traditional encryption schemes, the aforementioned feature is not available. However, one can see from Figure 10 that when size of DCT block reduces, decryption quality also reduces.

5. Comparison with Other Traditional Image Encryption Schemes

In this section, the proposed encryption scheme is compared with other state-of-the-art encryption algorithms. As cameraman (shown in Figure 11) image is most widely used in the area of image processing and image security, we have considered cameraman image in this section. The size of the cameraman image is 256 × 256 in this paper. Table 12 shows that the proposed technique outperforms other encryption techniques in all security metrics except MD and ID where the MD and ID are in favor of reference [38]. However, only these two metrics are not sufficient for the security. Results of all other security metrics show that the proposed technique is secure and real-time applicable.

6. Conclusion

A novel chaos-based encryption scheme is presented in this paper which can be deployed in the application of camera-based real-time secure occupancy monitoring system. The system initially transforms plaintext image to DCT coefficients and then a block from the coefficients is selected for confusion-diffusion processes. The ciphertext image size is obviously much smaller than the plaintext size, and hence the compressed ciphertext can be transmitted over a bandwidth-constrained channel. Experimental results reveal that the proposed encryption-compression system reduces overhead for channels and the ciphertext is also highly secure. Moreover, the quality of reconstructed plaintext image reduces with the size reduction of DCT coefficients. Comparison with other schemes highlighted that the proposed scheme is highly secure against a number of attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Harish Kumar extends his gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant no. R.G.P. 2/132/42.

References

[1] K. Sun, Q. Zhao, and J. Zou, “A review of building occupancy measurement systems,” *Energy and Buildings*, vol. 216, Article ID 109965, 2020.

[2] J. Ahmad, H. Larijani, R. Emmanuel, M. Mannion, and A. Javed, “Occupancy detection in non-residential buildings–a survey and novel privacy preserved occupancy monitoring solution,” *Applied Computing and Informatics*, 2018.

[3] S. Aziz Shah, J. Ahmad, A. Tahir et al., “Privacy-preserving non-wearable occupancy monitoring system exploiting wi-fi imaging for next-generation body centric communication,” *Micromachines*, vol. 11, no. 4, p. 379, 2020.

[4] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, “A novel secure occupancy monitoring scheme based on multi-chaos mapping,” *Symmetry*, vol. 12, no. 3, p. 350, 2020.

[5] A. Priya, K. Sinha, M. P. Darshani, and S. K. Sahana, “A novel multimedia encryption and decryption technique using binary tree traversal, Lecture Notes in Electrical Engineering,” in *Proceedings of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017)*, pp. 163–178, Springer, 2019.

[6] M. Sankari and P. Ranjana, “Privacy-preserving lightweight image encryption in mobile cloud,” in *Emerging Research in Computing, Information, Communication and Applications*, pp. 403–414, Springer, NY, USA, 2019.

[7] P. Rashmi, M. C. Supriya, and Q. Hua, “Enhanced lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare,” *Security and Communication Networks*, vol. 2022, Article ID 9363377, 9 pages, 2022.

[8] X. Xun Yi, C. H. Chik How Tan, C. K. Chee Kheong Slew, and M. Rahman Syed, “Fast encryption for multimedia,” *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 101–107, 2001.

[9] R. Matthews, “On the derivation of a “chaotic” encryption algorithm,” *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[10] A. U. Rahman, K. Sultan, D. Musleh, N. Aldhafferi, A. Alqahtani, and M. Mahmud, “Robust and fragile medical image watermarking: a joint venture of coding and chaos theories,” *Journal of healthcare engineering*, vol. 2018, Article ID 8137436, 11 pages, 2018.

[11] A. Qayyum, J. Ahmad, W. Boulila et al., “Chaos-based confusion and diffusion of image pixels using dynamic substitution,” *IEEE Access*, vol. 8, 2020.

[12] X. Wang, L. Feng, R. Li, and F. Zhang, “A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model,” *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2797–2824, 2019.

[13] S. F. Raza and V. Satpute, “A novel bit permutation-based image encryption algorithm,” *Nonlinear Dynamics*, vol. 95, no. 2, pp. 859–873, 2019.

[14] R. Vidhya and M. Brindha, “A chaos based image encryption algorithm using rubik’s cube and prime factorization process (cierpf),” *Journal of King Saud University-Computer and Information Sciences*, 2020, In press.

[15] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, “A robust image encryption scheme using chaotic tent map and cellular automata,” *Nonlinear Dynamics*, vol. 100, 2020.

[16] C.-F. Zhao and H.-P. Ren, “Image encryption based on hyper-chaotic multi-attractors,” *Nonlinear Dynamics*, vol. 100, no. 1, pp. 679–698, 2020.

[17] T. S. Ali and R. Ali, “A new chaos based color image encryption algorithm using permutation substitution and boolean operation,” *Multimedia Tools and Applications*, Springer, Berlin/Heidelberg, Germany, pp. 1–21, 2020.

[18] H. Liu, Y. Xu, and C. Ma, “Chaos-based image hybrid encryption algorithm using key stretching and hash feedback,” *Optik*, vol. 216, Article ID 164925, 2020.

[19] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, “An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata,” *Neural Computing & Applications*, vol. 32, no. 9, pp. 4961–4988, 2020.

[20] F. Musanna, D. Dangwal, S. Kumar, and V. Malik, “A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor,” *The Imaging Science Journal*, vol. 68, no. 1, pp. 24–40, 2020.

[21] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, “A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation,” *Optics & Laser Technology*, vol. 121, p. 105777, 2020.

[22] J. Karmakar and M. K. Mandal, “Chaos-based image encryption using integer wavelet transform,” in *Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 756–760, IEEE, Noida, India, February 2020.

[23] X.-H. Song, H.-Q. Wang, S. E. Venegas-Andraca, and A. A. Abd El-Latif, “Quantum video encryption based on qubit-planes controlled-xor operations and improved logistic map,” *Physica A: Statistical Mechanics and Its Applications*, vol. 537, Article ID 122660, 2020.

[24] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, “Provably-secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection,” *IEEE Transactions on Industrial Informatics*, vol. 16, 2020.

[25] X. Li, J. Niu, S. Kumari et al., “A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security,” *Wireless Personal Communications*, vol. 89, no. 2, pp. 569–597, 2016.

[26] X. Kang, Y. Chen, F. Zhao, and G. Lin, “Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain,” *Soft Computing*, vol. 24, no. 14, Article ID 10561, 2020.

[27] J. S. Khan, S. K. Kayhan, S. S. Ahmed et al., “Dynamic s-box and pwlcm-based robust watermarking scheme,” *Wireless Personal Communications*, vol. 125, pp. 1–18, 2022.

[28] N. A. Azam, U. Hayat, and M. Ayub, “A substitution box generator, its analysis, and applications in image encryption,” *Signal Processing*, vol. 187, Article ID 108144, 2021.

[29] J. Daemen and V. Rijmen, *The Design of Rijndael: The Advanced Encryption Standard (AES)*, Springer Nature, NY, USA, 2020.

[30] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, “A novel substitution box for encryption based on lorenz equations,” in *Proceedings of the 2017 International Conference on Circuits, System and Simulation (ICCSS)*, pp. 32–36, IEEE, London, UK, July 2017.

[31] T. K. Alshekly, E. A. Albahrani, and S. H. Lafta, “4d chaotic system as random substitution-box,” *Multimedia Tools and Applications*, vol. 81, pp. 1–22, 2022.

[32] W.-H. Wen-Hsiung Chen, C. Smith, and S. Fralick, “A fast computational algorithm for the discrete cosine transform,” *IEEE Transactions on Communications*, vol. 25, no. 9, pp. 1004–1009, 1977.

[33] J. Ahmad, S. O. Hwang, and A. Ali, “An experimental comparison of chaotic and non-chaotic image encryption schemes,” *Wireless Personal Communications*, vol. 84, no. 2, pp. 901–918, 2015.

[34] J. Ahmad and S. O. Hwang, “Chaos-based diffusion for highly autocorrelated data in encryption algorithms,” *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.

[35] J. Ahmad and S. O. Hwang, “A secure image encryption scheme based on chaotic maps and affine transformation,” *Multimedia Tools and Applications*, vol. 75, no. 21, Article ID 13951, 2016.

[36] J. Arif, M. A. Khan, B. Ghaleb et al., “A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution,” *IEEE Access*, vol. 10, Article ID 12966, 2022.

[37] F. E. Abd El-Samie, H. E. H. Ahmed, I. F. Elashry et al., *Image Encryption: A Communication Perspective*, CRC Press, Boca Raton, Florida, 2013.

[38] K. A. K. Patro, M. Prasanth Jagapathi Babu, K. Pavan Kumar, and B. Acharya, “Dual-layer DNA-encoding-decoding operation based image encryption using one-dimensional chaotic map,” *Advances in Data and Information Sciences*, vol. 94, pp. 67–80, 2020.

[39] A. Anees, A. M. Siddiqui, and F. Ahmed, “Chaotic substitution for highly autocorrelated data in encryption algorithm,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3106–3118, 2014.

[40] J. S. Khan and J. Ahmad, “Chaos based efficient selective image encryption,” *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.