Review Article

A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices

Sanaz Kavianpour,1 Bharanidharan Shanmugam,2 Sami Azam,2 Mazdak Zamani,3 Ganthan Narayana Samy,1 and Friso De Boer2

1Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia
2College of Engineering, Information Technology and Environment, Charles Darwin University, Darwin, Northern Territory 0909, Australia
3School of Arts and Sciences, Felician University, Lodi, New Jersey 07644, USA

Correspondence should be addressed to Bharanidharan Shanmugam; bharanidharan.shanmugam@cdu.edu.au

Received 5 April 2019; Revised 21 July 2019; Accepted 31 July 2019; Published 29 August 2019

Copyright © 2019 Sanaz Kavianpour et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things (IoT) has become one of the most significant technologies in recent years because of possessing the diverse application domains. The variety of applications results in a large amount of users’ private information diffusion that will pose a paramount security concern. User authentication is a significant factor in the IoT environment as it allows the user to communicate with the device securely. Integration of authentication technologies with IoT ensures secure data retrieval and robust access control. This paper provides a comprehensive systematic literature review of various authentication mechanisms for IoT security proposed in the literature. With the comparison of existing authentication mechanisms that are developed for the IoT in terms of security via a multicriteria classification, the open issues that require further research are identified.

1. Introduction

Internet of Things (IoT) is a new paradigm where everyday objects are interconnected and communicate with each other over the Internet [1]. IoT facilitates a direct integration of physical objects with the cyber world through smart sensors, RFID tags, smartphones, and wearable devices [2]. IoT networks offer various application domains encompassing environmental monitoring, healthcare, smart cities, military affairs, and intelligent transportation system [3, 4]. IoT application will improve rapidly. Cisco systems predict that by 2020, there will be over 50 billion connected things in the Internet consist of sensors, actuators, GPS devices, mobile devices, and all other smart things [5]. The security and privacy of these devices are the most notable challenges in IoT [6]. These devices have an insufficient mechanism of computing platforms, and the communications are wireless often that prone the system to various attacks. Furthermore, the number of devices revealed to the public network are increasing gradually and the devices have direct interaction with the physical world to gather data. All these make them a suitable target for malicious users. Hence, it is substantial to assure devices’ authenticity to ensure that the legal device is operating in an expected status and is not affected by malware. As IoT devices are built on various technologies such as power management and sensors, their security requirements vary from one application to another. Several security requirements, which are required to be considered in designing an authentication protocol in IoT perimeter, are delineated in Figure 1.

IoT development is based on wireless networks that collect information for authorised users. In a wireless network, the instructions are sent to terminal nodes by the platform, and the information is collected and transmitted to the platform by the terminal nodes [7]. Mutual authentication is required for the communication process to ensure the security of the network. It hinders illegal adversaries to use the network for malicious tasks. Moreover, other nodes
Ensures the data protection transmitting between the communicating parties from unauthorised access.

Integrity
Ensures that the generated data by IoT sensors should not be altered in transit and should not be compromised while retaining at the big data warehouse.

Authentication
Enables the IoT devices to verify the communicating peer identity.

Availability
Enforces the continuous availability of IoT devices to the user when it is required.

Data freshness
Ensures that each data set is sent by the IoT devices is fresh and no adversary replays with the old messages.

Non-repudiation
Demonstrates that a communicating party cannot disprove sending of an earlier message.

Authorization
Ensures that merely authorised communicating parties are authorised to access the various resources services.

Resilience against sensing device capture attack
Ensures other parts of the devices and network resources are protected by security mechanism if some parts are compromised.

Unbreakable service
Enable strong deployed mechanism that provides continuous services in case of energy issues or physically stolen of devices by the adversary.

Forward secrecy
Generating random public key each session to hamper the one compromised message to affect other messages.

Anonymity
Enforces that the information of a legal party can not be accessed by an attacker.

Attack resistance
Ensures secure authentication process against various potential attacks.

Scalability
Ensures authentication scheme is scalable enough to add nodes dynamically. The computational workload should not be affected by the enhancement number of devices.

2. Research Method

A systematic literature review (SLR) is employed to review the existing documents about authentication mechanisms in IoT and discuss the results of the conducted review to conduct further research if it is required. Kitchenham and Charters [16] defined SLR as a means of identifying, evaluating, and interpreting all available research relevant to a particular research question, topic area, phenomenon of interest. da Silva et al. [17] stated incorporating current work towards the research questions addressed by this research are as follows:

RQ1. What are the security threats in the IoT perimeter?
RQ2. What are the IoT authentication schemes security issues/challenges?
RQ3. What kind of authentication scheme (techniques) has been developed or applied for IoT-based architectures?
RQ4. What kind of security evaluation is used for IoT authentication?

2.2. Search Process. The search process is as follows. Primary search process consists of searching research keywords (authentication, CPS, IoT, and lightweight) through search engines such as ACM Digital Library, IEEE Xplore, and ScienceDirect. Secondary search process comprises searching of publications manually in the relevant area of research.

2.3. Inclusion and Exclusion Criteria. The papers that describe research on authentication schemes for IoT are included in our review. Papers with respect to their years,
metrics, techniques, evaluation criteria, and results have been examined. The inclusion of papers was based on the similarity of the research with IoT authentication scheme topic. The papers that did not describe security experimental results were excluded from the review.

3. Results of the Systematic Literature Review

In this section, the result of our SLR is formulated. The results focus the set answers to the questions taken as bottom-line of our systematic literature review. Each subsection provides information to answer these questions regarding the objective of the studies. Different tables are shown to represent the results of this review. Authentication schemes in IoT showing the distribution of studies per year and publication source are investigated.

3.1. RQ1: What Are the Security Threats in the IoT Perimeter? The presence of IoT devices in unprotected perimeters escalates the necessity of considering all possible security threats that can compromise the devices. Security threats in the IoT networks are described in Figure 2.

3.2. RQ2: What Are the IoT Authentication Schemes Security Issues/Challenges? Table 1 illustrates the cloud-driven IoT authentication schemes’ security issues/challenges with the proposed solutions [18–22].

3.3. RQ3: What Kind of Authentication Scheme (Techniques) Has Been Developed or Applied for IoT-Based Architectures?

3.3.1. Cloud-Based IoT Authentication. Cloud can be a proper platform for storing and processing the IoT devices data. Cloud computing and IoT integration affect our daily life tasks impressively. Cloud-driven IoT privileges are more than a generic IoT architecture. Processing the real-time queries can be performed with less cost and alleviated processing overhead by cloud-driven IoT [18]. In network architecture, a remote object/user should verify itself within the IoT and cloud architecture. Hence, the authentication scheme is required. Table 2 summarizes the relevant schemes based on IoT-cloud architecture authentication.

A cloud-based platform can be employed as a big data warehouse for IoT data. In IoT-based critical applications, only authorised users can access the IoT sensors data or query stored data on cloud servers to realise the hidden patterns of some phenomena. Wazid et al. [37] discussed the authentication schemes for cloud-driven IoT-based big data environment and provided a comparative study of numerous existing authentication schemes that are shown in Table 3.

3.3.2. Lightweight Authentication. A lightweight and secure authentication scheme is required because of the above-mentioned weaknesses in the IoT-cloud architecture schemes. Feng et al. [44] presented a lightweight mechanism for Attestation and Authentication of Things (AAoT), which provides software integrity, mutual authentication, and tamper-proof feature for software-based embedded devices. This scheme relies on physical unclonable functions (PUFs). Both strong PUFs and weak PUFs are used by the protocol. PUF-based memory random filling is employed to alleviate the memory resources. The scheme delineates efficient implementations and optimizations for each of the building blocks of AAtT and provides mutual authentication.

(1) Attestation. The identity authenticity and software integrity of connected smart embedded devices require to be guaranteed to hinder malicious nodes. The identity authenticity ensures that the device is a legitimate one, and the software integrity ensures the device status and expected behaviors. The identity and integrity of devices can be verified by a known protocol as attestation [45]. Two types of attestation for low-resource devices are software-based attestation [46–49] and attestation based on minimal embedded security architecture [50–52]. These methods are ineffective if IoT devices are impersonated. They are based on the traditional secure storage technology that is costly, rigid, and unsafe [53, 54]. Software-based attestation methods are as follows:

(a) Time-Based Attestation. It is the most regular method such as SWATT [46], Pioneer [55], and
SCUBA [47]. It performs the checksum computation over the program memory that specifies time delays in case of memory alteration. (b) **Attestation Based on Memory Filling.** Attackers may elicit the extra memory space. Filling the empty memory by noncompressible pseudo-random noises was proposed by researchers [56–58]. Memory printing [59] and quine [60] can also be used to fill the RAM space. Time-based attestation and attestation based on memory filling are vulnerable to offline static analysis, reverse engineering, and manipulation due to the fixed function. (c) **Attestation Based on Random Construction of Attestation Function.** Shaneck et al. [61] proposed a random attestation function by a verifier that is sent to a prover per-protocol run. Park and Shin [62] proposed a novel randomized hash function tailored to low-cost CPUs, which was infeasible due to the network bandwidth consumption and complexity. Software-based attestation is not robust against the following attacks: memory copy attack, proxy attack Pioneer [55], an attack via the address translation mechanisms [63], the code compression attack [64], and attack exploiting high execution-time variance [65]. Hence, the software-based attestation security is polemic. (d) **Embedded Security Architecture and Attestation.** Recent research is based on a hardware-software codesign such as SMART [60] or TrustLite [51]. The goal is to make a dynamic trust anchor in a constrained embedded device. The trust anchor established can be further used to design a scalable collective attestation fulfill security requirements. Previous attestation methods were focused on software attacks. (2) **Authentication.** Traditional authentication method employs a cryptographic logic with a secret key that lacks secure hardware features and has a high cost. PUFs implemented a secure lightweight device authentication by exploiting the unavoidable manufacturing variations of an integrated circuit to generate a unique device fingerprint. PUF-based authentication is robust due to the fact that tampering with the PUF would render it useless.

<table>
<thead>
<tr>
<th>Issues/challenges</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited computation power and memory storage</td>
<td>The processing capability of IoT devices such as sensors does not have strength in terms of speed. Also, restricted memory storage makes IoT devices incapable of performing operations with high computational power. Some devices have confined battery backup that switches to the power saving mode to save energy when there is no activity. The battery backup restrictions cause difficulty in providing adequate security.</td>
<td>Design a user authentication scheme for IoT by employing lightweight cryptographic operations such as the Advanced Encryption Standard (AES) algorithm and cryptographic one-way hash function.</td>
</tr>
<tr>
<td>Energy requirement</td>
<td></td>
<td>Design a lightweight cryptography authentication scheme.</td>
</tr>
<tr>
<td>Scalability</td>
<td>The number of IoT devices enhances gradually.</td>
<td>Design an authentication scheme with the functionality of smart sensing device augmentation.</td>
</tr>
<tr>
<td>Mobility</td>
<td>Some devices are mobile such as a wearable sensing device that monitors a person temperature. These devices are connected to different networks based on the user location, which require various security configuration and settings.</td>
<td>Develop a mobility-compliant security technique and interoperability among networks.</td>
</tr>
<tr>
<td>Support for heterogeneous devices</td>
<td>Various devices such as a sensor or RFID tags have a different capability of computation, memory, and embedded software. If a new smart device is added or removed, other entities should be notified through the trusted authority to update this in their memory to prevent security vulnerability.</td>
<td>Design a lightweight authentication scheme.</td>
</tr>
<tr>
<td>Dynamic security updates</td>
<td></td>
<td>Employ P2P networks and develop mutual authentication mechanisms.</td>
</tr>
<tr>
<td>Protection against physical capturing</td>
<td>The number of IoT devices enhances gradually.</td>
<td>Design the authentication scheme in which in case of a stolen device, the security of other parts does not get affected. Employing tamper-resistant packaging can be useful.</td>
</tr>
<tr>
<td>Security and privacy</td>
<td></td>
<td>Apply machine-learning approaches to avoid data leakage.</td>
</tr>
</tbody>
</table>
authentication strengthens authentication protocols due to the singularity, reproducibility properties, and unclonability. There are two types of PUFs as weak and strong PUFs [66]. Kong et al. [67] presented a PUFatt as a novel PUF design (called ALU PUF) in regards to the delay difference in two different

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Method</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liao and Wang [23]</td>
<td>Multiserver architecture authentication scheme with the dynamic identity concept. The secure dynamic id improvement according to the remote user authentication scheme in a multiserver environment.</td>
<td>Vulnerable to user and server forgery attacks.</td>
</tr>
<tr>
<td>Le et al. [26]</td>
<td>Employing smart cards in a multiserver architecture.</td>
<td>Vulnerable to impersonation attack, offline password guessing attack, etc.</td>
</tr>
<tr>
<td>Li et al. [27]</td>
<td>Employing smart cards as a secure dynamic id-based remote authentication scheme for distributed systems.</td>
<td>Vulnerable to offline password guessing attack if smart card loss.</td>
</tr>
<tr>
<td>Xue et al. [29]</td>
<td>A pseudonym identity-based authentication with key agreement protocol.</td>
<td>Inadequate identity-hidden feature and vulnerable to the offline password guessing attack.</td>
</tr>
<tr>
<td>Shunmuganathan et al. [30]</td>
<td>Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple server architecture.</td>
<td>The user tracking attack could affect for multiserver framework.</td>
</tr>
<tr>
<td>Zhu [31]</td>
<td>Using an improved smart card authentication scheme.</td>
<td>Vulnerable to offline password guessing attack.</td>
</tr>
<tr>
<td>Li et al. [32]</td>
<td>Applying the anonymous-based authentication key agreement in the multiserver architecture.</td>
<td>Vulnerable to user tracking and insider attack.</td>
</tr>
<tr>
<td>Maitra et al. [34]</td>
<td>Employing password and smart card: cryptanalysis and design.</td>
<td>Vulnerable to the offline guessing and user tracking attack.</td>
</tr>
<tr>
<td>Amin et al. [35]</td>
<td>A lightweight authentication protocol for IoT-enabled devices in a distributed computing environment.</td>
<td>Vulnerable to the offline guessing attack and does not satisfy audit property.</td>
</tr>
<tr>
<td>Zhou et al. [36]</td>
<td>Employing a lightweight two-factor authentication scheme that consists of one-way hash function and exclusive-or operation with cloud assistance.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Description</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yeh et al. [38]</td>
<td>Employing elliptic curve cryptography (ECC) for user authentication in wireless sensor networks (WSNs).</td>
<td>Not support mutual authentication.</td>
</tr>
<tr>
<td>Turkanović et al. [39]</td>
<td>User authentication and key agreement scheme for heterogeneous wireless sensor networks.</td>
<td>Vulnerable to offline password and identity guessing.</td>
</tr>
<tr>
<td>Hsieh and Leu [40]</td>
<td>Employing an authentication scheme for WSNs, which can be applicable for IoT as well.</td>
<td>Vulnerable to an insider, offline guessing, user forgery, and sensor node physical capture attack. Not providing session key security and mutual authentication.</td>
</tr>
<tr>
<td>Farash et al. [41]</td>
<td>User authentication and key establishment for a heterogeneous architecture of WSNs.</td>
<td>Vulnerable to password guessing in offline mode through the lost/stolen smart card, user impersonation, and session-specific temporary information leakage attack.</td>
</tr>
<tr>
<td>Challa et al. [42]</td>
<td>Authentication scheme based on ECC digital signature.</td>
<td>Inadequate computation and communication overheads in IoT.</td>
</tr>
<tr>
<td>Li et al. [43]</td>
<td>Authentication scheme based on ECC for industrial IoT.</td>
<td>Requires high computational overhead for the resource-constrained sensor nodes and cannot provide essential functionality features like the biometric update.</td>
</tr>
</tbody>
</table>
Henceforth, the user connects to the sought sensor node by protocol used a gateway node for the user registration first. Dhillon and Kalra [79] proposed a lightweight biometric multifactor remote user authentication scheme for IoT security. Schulz et al. [68] presented a decentralized authentication mechanism called bubbles of trust. They create bubbles in which things can identify and trust each other by using blockchain Ethereum that implements smart contracts. The Master (a device of the bubble) sends a transaction including the Master’s identifier and the group identifier. The uniqueness of both will be checked by the blockchain. The bubble will be created if the transaction is valid. In turn, the Followers (each object that makes part of the system) send transactions to the relevant bubbles. Every Follower has a ticket that consists of a groupID, an objectID, pubAddr, and a Signature structure (using elliptic curve digital signature algorithm (ECDSA). The uniqueness of the Follower’s identifier and the Follower’s ticket validity are verified by the smart contract. In case of an initial successful transaction, there is no need for latter authentication by the Follower.

Various research studies were done on the blockchains and IoT integration while few pieces of researches were on the blockchain’s application in meeting IoT security requirements. Table 5 outlines the researches that are mostly based on the security mechanism such as Bitcoin or Ethereum. Although these mechanisms ensure anonymity completely, there is no identification assurance as a fundamental requirement. Private blockchains should be used to ensure identification. These mechanisms have limitations such as the difficulty of inserting a new service or a device. No implementations or simulations were provided by these researches.

### Table 4: Developed attestation schemes and the drawbacks.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Description</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kong et al. [67]</td>
<td>PUFAtt links software-based attestation to fundamental device characteristics through a novel processor-based PUF, which provide a lightweight remote attestation scheme.</td>
<td>(i) Requires any hardware modifications. (ii) High computation and storage overhead. (iii) No real performance and implementation details of the integrated system. (iv) Does not support mutual authentication. (v) Vulnerable to modeling attacks by machine-learning techniques, and security protocols are unsafe.</td>
</tr>
<tr>
<td>Schulz et al. [68]</td>
<td>A lightweight remote attestation scheme that employs PUFs to connect software attestation to remotely identifiable hardware.</td>
<td>(i) Generating additional CRPs enhance the computational and communication difficulty that is not appropriate for low-end devices.</td>
</tr>
</tbody>
</table>

3.3.3. Decentralized Blockchain-Based Authentication.
Making an efficient centralized authentication system for IoT is not feasible because of IoT size and other features. Hammi et al. [69] presented a decentralized authentication mechanism called bubbles of trust. They create bubbles in which things can identify and trust each other by using blockchain Ethereum that implements smart contracts. The Master (a device of the bubble) sends a transaction including the Master’s identifier and the group identifier. The uniqueness of both will be checked by the blockchain. The bubble will be created if the transaction is valid. In turn, the Followers (each object that makes part of the system) send transactions to the relevant bubbles. Every Follower has a ticket that consists of a groupID, an objectID, pubAddr, and a Signature structure (using elliptic curve digital signature algorithm (ECDSA). The uniqueness of the Follower’s identifier and the Follower’s ticket validity are verified by the smart contract. In case of an initial successful transaction, there is no need for latter authentication by the Follower.

Various research studies were done on the blockchains and IoT integration while few pieces of researches were on the blockchain’s application in meeting IoT security requirements. Table 5 outlines the researches that are mostly based on the security mechanism such as Bitcoin or Ethereum. Although these mechanisms ensure anonymity completely, there is no identification assurance as a fundamental requirement. Private blockchains should be used to ensure identification. These mechanisms have limitations such as the difficulty of inserting a new service or a device. No implementations or simulations were provided by these researches.

3.3.4. Biometrics-Based Remote User Authentication Schemes (Multifactor Authentication). Dhillon and Kalra [79] proposed a lightweight biometric multifactor remote user authentication and key agreement scheme for IoT security. The protocol used a gateway node for the user registration first. Henceforth, the user connects to the sought sensor node by his smart device. The proposed multifactor biometric user authentication phases are as follows:

1. **User Registration Phase.** It consists of two phases after IoT deployment as the registration between the user and gateway node and the registration between the gateway node and the sensor node. Registration with the gateway node is required for access to IoT. The user executes the authentication phase to generate a shared session key. The second registration is required to add nodes dynamically to the network.

2. **Login Phase.** To initiate the authentication phase, the user should log in to the IoT services. Registration and authentication are based on the user biometrics and password.

3. **Authentication Phase.** The user and the node generate an encrypted secret session key that can be used onetime. There is mutual authentication between a remote user and the IoT node.

4. **Password-Change Phase.** The user needs to update his/her password periodically for security reasons.

Table 6 indicates various biometrics-based remote user authentication schemes that have been done by researchers. They mostly employ the cryptographic key establishment between the user and the gateway node.

3.4. **RQ4: What Kind of Security Evaluation is Used for IoT Authentication?** Security of an authentication scheme requires to be evaluated via various security analysis metrics to ensure that is not vulnerable to attacks. Formal security analysis should be performed to verify the scheme security.

3.4.1. **Proverif.** It is a formal verification tool that checks the security properties’ compatibility for cryptographic protocols [96]. Proverif patronages cryptographically operated symmetric encryption/decryption, hash functions, and bit-commitment. Generally, it is employed by researchers to evaluate security reachability, proving session key secrecy, and authentication.

In 2019, Zhou et al. [36] used Proverif to test their scheme security and robustness against common attacks. They employed the two most prevalent cryptotechniques for
Table 6: Biometrics-based remote user authentication schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Description</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Khan and Zhang [80]</td>
<td>Enhancing the security of a biometric authentication scheme. Providing comparison on the cost of two key agreement protocols as Kerberos and the Elliptic Curve Diffie–Hellman key exchange with authentication delivered by the elliptic curve digital signature algorithm (ECDH-ECDSA).</td>
<td>Does not provide mutual authentication, and it is vulnerable to server spoofing attacks.</td>
</tr>
<tr>
<td>de Meulenaer et al. [81]</td>
<td>Curve Diffie–Hellman key exchange with authentication delivered by the elliptic curve digital signature algorithm (ECDH-ECDSA). Proposing an authentication scheme based on a biometric and smart card that delivers less computational cost.</td>
<td>It can be applied only where a trusted third party is available. Furthermore, the energy cost of listening increases communication costs.</td>
</tr>
<tr>
<td>Li and Hwang [82]</td>
<td>Presenting user authentication and key agreement schemes for WSN. Proposing an electrocardiogram-signal-based protocol using biometric encryption to provide mutual authentication.</td>
<td>There is no mutual authentication, and it is not robust against attacks.</td>
</tr>
<tr>
<td>He et al. [83]</td>
<td>Providing an authentication framework considering password, smart card, and biometrics. Improvement of an effective biometric-based authentication scheme employing smart cards and its analysis in terms of security.</td>
<td>An insufficient balance between safety and security.</td>
</tr>
<tr>
<td>Yao et al. [84]</td>
<td>Presenting an authentication and access control in the IoT. Proposing a multifactor scheme employing biometric, password, and random nonce generated by the user and server.</td>
<td>Lack of threat identification in the provided framework.</td>
</tr>
<tr>
<td>Huang et al. [85]</td>
<td>Proposed a two-way IoT security architecture in which authentication is provided by datagram transport Layer security handshake.</td>
<td>Susceptible to impersonation and gateway node bypassing attack.</td>
</tr>
<tr>
<td>An [86]</td>
<td>Presenting an authentication framework considering password, smart card, and biometrics. Improvement of an effective biometric-based authentication scheme employing smart cards and its analysis in terms of security.</td>
<td>Supporting just it, DTCT, SSR, and PP partly.</td>
</tr>
<tr>
<td>Kothmayr et al. [87]</td>
<td>Presenting a multifactor scheme employing biometric, password, and random nonce generated by the user and server.</td>
<td>The high cost of message exchange and inadequate security.</td>
</tr>
<tr>
<td>Liu et al. [88]</td>
<td>Proposing a two-way IoT security architecture in which authentication is provided by datagram transport Layer security handshake.</td>
<td>Insufficient security advancement.</td>
</tr>
<tr>
<td>Li et al. [89]</td>
<td>Presenting user authentication and key agreement schemes for WSN. Proposing an electrocardiogram-signal-based protocol using biometric encryption to provide mutual authentication.</td>
<td>There is no mutual authentication, and it is not robust against attacks.</td>
</tr>
</tbody>
</table>
secure communications as the AES and SHA-2 (256 bits) algorithms. Arduino Uno platform was used with the implementation of SHA-3 (512-bits). The results delineate that their scheme is practical to be implemented for IoT devices. Table 7 illustrates the comparison of this scheme with another two relevant ones. In terms of security and efficiency, [43] delineates superior results than the other two schemes.

Hammi et al. [69] applied Ethereum as blockchain and developed the smart contract to ensure the scheme functionality. They encode and decode Ethereum data for the interactions between end nodes and the blockchain using a C++ interface. The comparison of [69] with other authentication schemes based on association phase is described in Table 8. The evaluation was based on the execution time, energy consumption, and financial cost. In regards to constrained devices, the fewer number of messages denotes minor system’s consumption. If the implementation is on the same hardware, energy, and computation consuming will be alleviated. Additionally, Messages’ authentication is realised by the ECDSA. Message authentication required time is based on the employed blockchain compared to other schemes, which is in some milliseconds. This scheme provides a robust identification, authentication, data integrity, and availability. The evaluation results delineate that this scheme ensures the security requirements as well as resiliency toward attacks. This scheme cannot be employed in actual applications, and it has costs due to the cryptocurrency used by the blockchain system.
| Scheme                  | Mutual Authentication | Key agreement | User anonymity | Password change | Replay attack | Impersonation attack | Password change attack | Parallel session attack | Gateway node bypassing attack | Smart card/smart device stolen attack | Man-in-the-middle attack | Denial-of-service attack |
|------------------------|-----------------------|---------------|----------------|----------------|---------------|-----------------------|------------------------|-------------------------|-------------------------------|-------------------------------|--------------------------|
| He et al. [83]         | ✗                     | ✗             | ✓              | ✓              | ✓             | ✓                     | ✗                      | ✓                       | ✗                             | ✗                             | ✗                        | ✗                       |
| An [86]                | ✗                     | ✓             | ✗             | ✗             | ✗             | ✗                     | ✗                      | ✗                       | ✗                             | ✗                             | ✗                        | ✗                       |
| Xue et al. [91]        | ✓                     | ✓             | ✓             | ✓             | ✓             | ✓                     | ✓                      | ✗                       | ✗                             | ✗                             | ✓                        | ✓                       |
| Turkanović et al. [39] | ✓                     | ✓             | ✓             | ✓             | ✓             | ✓                     | ✓                      | ✓                       | ✓                             | ✓                             | ✓                        | ✓                       |
| Chen et al. [94]       | ✗                     | ✗             | ✓             | ✗             | ✗             | ✗                     | ✗                      | ✗                       | ✗                             | ✗                             | ✗                        | ✗                       |
| Das and Goswami [95]   | ✓                     | ✗             | ✗             | ✓             | ✗             | ✗                     | ✗                      | ✗                       | ✗                             | ✗                             | ✗                        | ✓                       |
| Dhillon and Kalra [79] | ✓                     | ✓             | ✓             | ✗             | ✓             | ✓                     | ✓                      | ✓                       | ✓                             | ✓                             | ✓                        | ✓                       |
3.4.2. **Burrows–Abadi–Needham (BAN) Logic.** A set of rules that can be used to analyze the authentication protocols are known as BAN logic [41]. Through BAN logic, the communicating parties can specify the trustworthiness of the exchanged messages and mutually authenticate each other in IoT perimeter.

3.4.3. **Real-or-Random (ROR Model).** The ROR model can be used to authenticate key exchange protocols.

3.4.4. **Automated Validation of Internet Security Protocols and Applications (AVISPA).** A software tool that attests the resilience of an authentication scheme against replay and man-in-the-middle attacks [99]. It analyzes large-scale Internet security protocols and applications. High-Level Protocol Specification Language (HLPSL) is employed to code the protocols.

   The proposed authentication scheme by Dhillon and Kalra delineates robustness against numerous attacks that are depicted in Table 9. This scheme provides mutual authentication and a secure key as well as ensures password protection. The scheme security analysis is performed through formal verification using the AVISPA tool, which ensures its security if it is compromised.

3.4.5. **Cryptographic Protocol Shapes Analyzer (CPSA).** CPSA is an analysis tool comprising authentication tests that count indispensable various cryptographic protocol executions [100]. It is based on a Dolev-Yao model considering an intruder with unlimited access that can specify authentication as well as secrecy properties.

   Feng et al. [44] analyzed the AAoT protocol security using the CPSA tool. The experimental results delineate the mutual authentication as well as the secrecy of CRPs and PUFRoT within the authorization protocol. In AAoT, the possibility of memory copy attack is substantial as a valid checksum cannot be counterfeited [44]. AAoT is robust against cloning or impersonating because of the PUF uncloneability and unpredictability. A cloned or impersonated prover requires access to the PUF CRPs or keys from the legitimate prover device to fraud verifier.

   Table 10 demonstrates the comparison result of AAoT scheme with the most two similar approaches by [67, 68]. The concentration of AAoT is on static attestation. Additional techniques are required for runtime protection such as control flow attestation. AAoT is applicable for low-resource devices. To secure the IoT and CPS, the integration of attestation and authentication can be practical. AAoT ensures either integrity or authenticity and removes the gap from the protocol theory to tangible realization. The AAoT covers the problems in PUFatt.

### Table 10: Comparison of evaluation performance.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Supported PUF type</th>
<th>CRPs number</th>
<th>Hardware modifications</th>
<th>Implementation</th>
<th>Evaluation on the system</th>
<th>Mutual authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schulz et al. [68]</td>
<td>Strong PUFs</td>
<td>Iteration</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Kong et al. [67]</td>
<td>Strong PUFs</td>
<td>Iteration</td>
<td>✓</td>
<td>ALU PUF</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Feng et al. [44]</td>
<td>Strong PUFs and weak PUFs</td>
<td>2</td>
<td>×</td>
<td>SRAM PUF</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

4. **Discussion**

The IoT-based perimeters security issues and challenges that are required for authentication techniques are discussed. Furthermore, various existing authentication mechanisms for IoT are reviewed and compared. For instance, in [79] a lightweight authentication scheme uses one-way hash, perceptual hash functions, and XOR operations that are inexpensive. Hence, this scheme is appropriate for resource-constrained IoT devices. Although this scheme depicts robustness against various security attacks through AVISPA tool, it requires to be set up on a testbed to detect the memory requirements and its applicability for real IoT devices.

To secure IoT and CPS, integration of attestation and authentication is so significant and effective. Most of the existing schemes only render one of them. In [44], a lightweight attestation and authentication of low-resource things in IoT and CPS called AAoT are proposed. This scheme presents a feasible and secure hardware-software codesign employing the present resources limited in the smart embedded devices. AAoT integrity and authenticity are achieved by memory-based attestation and PUF-based authentication. In [43], a lightweight IoT-based authentication scheme in cloud computing circumstance presents robustness against different types of attacks and provides mutual authentication. The performance evaluation of this scheme delineates a highly suitable authentication scheme for real IoT-cloud circumstances. A decentralized blockchain-based authentication system for IoT called bubbles of trust is presented in [69]. Devices can communicate securely in the created virtual zones. Despite satisfying security requirements due to using a public blockchain and resilience toward attacks, it has three significant issues as follows: inadequate to real-time applications, requiring an initial phase, and cryptocurrency rate transformation.

Our findings demonstrate that various types of solutions have been proposed to address the secure authentication scheme for IoT. Even though the existing authentication schemes are applicable in IoT perimeter, there is still a gap, which necessitates additional effort in designing and developing a more secure authentication mechanism to hinder.
security breaches. The collected information from this SRL will assist future researchers by providing different directions to cover the gap and design a secure authentication scheme for IoT.

5. Conclusions

A massive heterogeneous network of IoT devices generates a huge amount of data that must be reachable and can be retrieved by only authorised user. Attack surfaces increase swiftly by the connection of billions of IoT devices. To provide secure access to the devices, services, and communication exchanges, authentication is a challenging task. Researchers proposed various authentication schemes, which might be different from each other and applicable across different domains. This paper reviewed different ways to perform authentication in IoT perimeters to identify the challenges and opportunities. The representative security requirements, security issues, and challenges of authentication schemes for IoT have been discussed. Various authentication schemes such as cloud-based IoT, lightweight, decentralized blockchain-based, and biometrics-based remote user authentication (multi-factor) were analyzed. Furthermore, the formal verification analysis provided by the different verification tools comprising Proverif, BAN logic, ROR model, AVISPA, and CPSA for evaluating the security of the authentication schemes is described. Although these authentication schemes for IoT have resulted in more secure design, they still have limitations, which require massive improvement to ensure deeper privacy and security. It is significant that the authentication scheme will be able to provide high security for IoT. Hence, a more in-depth investigation is necessitated in this direction, as achieving a robust authentication scheme is still an open issue.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References


