


Research Article

Safety Management Solution for Health Monitoring User Terminals Based on Trusted Computing

Maomao Liu ¹, Liping Wu,¹ Xingbo Zhang,¹ and Yan Li²

¹College of Information Science and Engineering, Shandong Agriculture and Engineering University, Jinan 250000, China

²Laboratory Management Center, Shandong Agriculture and Engineering University, Jinan 250000, China

Correspondence should be addressed to Maomao Liu; z2013459@sdaeu.edu.cn

Received 23 December 2021; Revised 8 February 2022; Accepted 11 February 2022; Published 2 March 2022

Academic Editor: Sheng Bin

Copyright © 2022 Maomao Liu 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.

The safety hazards of the monitoring platform must be solved to ensure the safety of health monitoring user terminals (HMUTs). To accurately measure the safety level of the safety management system, it is necessary to carry out effective trusted computing. However, the current trusted computing often ignores the subjectivity and personalization of trust, failing to consider the influence of privacy leak on trust. To solve these problems, this paper explores the safety management solution for HMUTs based on trusted computing. Specifically, the authors established a multidimensional trusted computing model for HMUTs, detailed the computing method for composite trust based on single-dimensional trust, and presented a trust management scheme for HMUTs. Experimental results demonstrate the feasibility and effectiveness of our model. Our research keeps up with the latest development trend of trusted computing and lives up to the trust and efficiency requirements of the collaborative processing mechanism for HMUT safety management.

1. Introduction

If health problems can be prewarned, passive treatment could be replaced with timely intervention before the problems occur. This would prevent tragedies like major personal accidents [1–6]. In recent years, intelligent products capable of actively monitoring health anywhere, anytime have attracted much attention [7–12]. These products collect various human health data via user terminals. The massive interactive data provide precise, timely, and complete feedback for hierarchical management of the life safety and physical health of people in a region [13–15]. The safety management of user terminals, which aims to ensure the trustworthiness of user identity and the completeness of user computing platforms, faces some hidden hazards. However, the massive number of users and insane volume of interactive data bring safety problems to user behaviors. To solve the problems, it is necessary to overcome the complex safety hazards faced by health monitoring platforms [16–20].

Kamble and Bhutad [21] proposed a health monitoring system for the elderly, which utilizes various sensors to monitor the physiological parameters of the patient,

including temperature, heartbeat, and electrocardiogram. Upon detecting any abnormal sign or symptom, the system will notify the caregiver via short message service (SMS) or e-mail. Ray and Ray [22] relied on exponential moving average (EMA) to adjust the output signal of the sensor array, encrypted the adjusted signal, and transmitted the encrypted signal to the connected fog node. Then, an algorithm was designed to push the data to the cloud platform for monitoring human activities and diseases. Jiang and Liu [23] developed a health monitoring system with lightweight security and privacy protection. The location and health information are acquired by dual-band radiofrequency identification (RFID), virtual path positioning algorithm, and RFID-based diet and motion data acquisition technology. Ahmid et al. [24] presented an intelligent patient monitoring system for automatic monitoring of patient's heart rate. The system operates more intelligently than the other systems: it keeps the confidentiality of authentication, authorization, and data sensing; after predicting the critical situation, it will send a message to the patient's family members, doctors, nurses, and hospital leaders, and trip an alarm. To solve the transmission delay of monitored data on

patient's health to the cloud, Kesavan and Arumugam [25] put forward a four-stage approach, including data acquisition, fog-to-cloud, decision-making, and execution, and demonstrated the high precision, good efficiency, quick response, and low computing cost of the approach in medical care. According to the structure and energy features of the medical objects, Somaya and Tomadar [26] studied the possibility of safe communication between medical tools within the hospital and devised a safe structure for their interfaces, using the safe mechanism provided by communication technologies, networks, and protocols. Wearing and Dragoni [27] comprehensively considered the key safety and privacy issues in family health monitoring systems and constructed a real-world sensor network for healthcare in the network environment.

After reviewing the relevant literature, it was discovered that the current trusted computing often ignores the subjectivity and personalization of trust, failing to consider the influence of privacy leak on trust. Besides, the untrusted probability is confused with uncertain probability in the result of traditional trusted computing. To solve the above problems, this paper updates the trusted computing method for HMUT safety management. The main contents are reported in Sections 2 and 3. Section 2 establishes a multidimensional trusted computing model for HMUTs and details the computing method for composite trust based on single-dimensional trust. Section 3 presents a trust management scheme for HMUTs and provides a trust management service capable of managing the trust of multiple HMUTs. Experimental results demonstrate the feasibility and effectiveness of our model.

2. Multidimensional Trusted Computing Model

The proposed trusted computing model for HMUTs was introduced from multiple dimensions. Figure 1 shows the framework of our multidimensional trusted computing model. As shown in that figure, the model consists of user terminals, an access network, platform servers, and a safety management layer. The user terminals refer to HMUTs like intelligent wearable devices.

To evaluate the ability of HUMTs to collaboratively complete health monitoring tasks, this paper introduces a parameter called competence trust (CT), which effectively reduces the probability for low competitive terminals to participate in health monitoring tasks. The CT of an HUMT depends on the requirements of the specific health monitoring task. Let ML_r^{RE} be the available information resources required by the health monitoring task; YZ_e^{RT} be the minimum threshold of the various information resources required to complete the current health monitoring task; ξ_l be the l information resources required to complete the pending health monitoring task. Then, we have

$$\begin{aligned} ML_r^{RE} &= \{\tau_1, \tau_2, \dots, \tau_k \dots \tau_m\}, \\ YZ_e^{RT} &= \{\xi_1, \xi_2, \dots, \xi_l \dots \xi_m\}. \end{aligned} \quad (1)$$

Each information resource of YZ_e^{RT} is divided by the corresponding information resource in ML_r^{RE} . The minimum

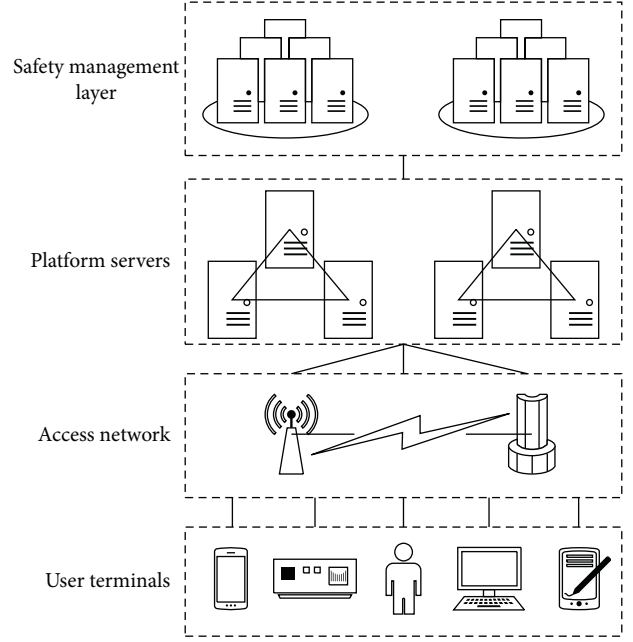


FIGURE 1: Framework of multidimensional trusted computing model.

ratio thus obtained is defined as the competence matching degree. That is, the information resource weakness of a terminal is defined as the matching degree between the information resources required to complete the health monitoring task and those possessed by the terminal, that is, the matching degree between YZ_e^{RT} and ML_r^{RE} . Since the competence matching degree should be smaller than 1, it is determined as the smaller value between 1 and the minimum ratio.

$$AM_{e,r} = \min \left(1, \min \left\{ \frac{\tau_1}{\xi_1}, \frac{\tau_2}{\xi_2}, \dots, \frac{\tau_l}{\xi_l}, \dots, \frac{\tau_m}{\xi_m} \right\} \right). \quad (2)$$

Furthermore, Shannon's information entropy was introduced to evaluate the CT of HMUTs, aiming to illustrate uncertain health monitoring information. Based on the entropy theory, the information entropy of event occurrence probability o can be calculated by

$$IE(o) = -o \cdot \log_2(o) - (1-o) \log_2(1-o). \quad (3)$$

The information entropy can increase the accuracy of CT evaluation of terminals and effectively quantify the risk of health monitoring tasks brought by low-competence users, making multidimensional trusted computing model more universal.

Since function (3) changes nonmonotonically, the CT function $SU_{e,r}$ directly corresponding to the monotonic interval of trust can be defined to convert the uncertain competence of terminals into CT.

$$SU_{e,r} = \begin{cases} \frac{IE(AM_{e,r})}{2}, & AM_{e,r} \in [0, 0.5), \\ 1 - \frac{IE(AM_{e,r})}{2}, & AM_{e,r} \in [0.5, 1]. \end{cases} \quad (4)$$

Figure 2 shows the flow of trusted computing of user terminals. To realize the safety management of HMUTs, it is necessary to establish the relationship between user terminals, which must collaborate with each other to complete complex tasks. In actual situation, HMUT M_r receives a few auxiliary information from the other peripheral devices. To evaluate the performance of HMUT M_e in the latest collaboration, it is assumed that HMUT M_r is independent of the auxiliary information from the other peripheral devices. The time window Δh representing the maximum number of historical collaborative tasks can be configured based on task density. Then, the set of probability scores based on time series can be expressed as

$$g_{e,r}(\Delta h) = \{t_{e,r}^1, t_{e,r}^2, \dots, t_{e,r}^l, \dots, t_{e,r}^{\Delta h}\}, \quad (5)$$

where $t_{i,j}^l \in [0, 1]$ is positively correlated with the degree of completion of historical tasks. For a user terminal, the stronger the competence, the better the performance.

The older the historical collaboration record, the less effective the information provided by the record. Let h be the current time; $h_{i,r}$ be the historical record; $t_{e,r}^l$ be the time of the historical record. Then, the time attenuation factor was introduced to the proposed trusted computing model.

$$\zeta_l = e^{-\left(h - h_{i,r}\right)}. \quad (6)$$

Time attenuation was performed on each historical record to improve the accuracy of trusted computing. Specifically, each record is updated by multiplying with the time attenuation factor.

$$t_{e,r}^l = t_{e,r}^l \times \zeta_l. \quad (7)$$

Beta distribution depicts the distribution of a single variable. It can be adopted as the prior distribution of binomial distribution. Thus, our model adopts beta distribution as the prior distribution of the success rate of the collaborative tasks between HMUTs. Suppose the past behaviors of user terminals are similar to their future behaviors. Let $\beta_{e,r}(\Delta h)$ and $\delta_{e,r}(\Delta h)$ be the number of positive records and that of negative records, respectively. The former records serve as positive evidence, and the latter as negative evidence. The corresponding probability model can be constructed based on the mathematical expectation of the beta distribution.

$$\begin{aligned} GS_{e,r}(\Delta h) &= \frac{\beta_{e,r}(\Delta h) + 1}{\beta_{e,r}(\Delta h) + \delta_{e,r}(\Delta h) + 2}, \\ \beta_{e,r}(\Delta h) &= \left(\sum g_{e,r}(\Delta h)^+\right), \\ \delta_{e,r}(\Delta h) &= \left(\sum g_{e,r}(\Delta h)^-\right). \end{aligned} \quad (8)$$

Formula (8) shows the historical records of collaboration between user terminals can be divided into $\beta_{e,r}(\Delta h)$ and $\delta_{e,r}(\Delta h)$.

Considering the dynamicity and instability of HMUTs, it is necessary to effectively identify the abnormal terminals. Otherwise, it would be impossible to realize accurate and

robust trusted computing, not to mention the optimization of direct trust. For this purpose, a penalty regulator λ_1 and a dynamic adaptor λ_2 were added.

$$\begin{aligned} GS_{e,r}(\Delta h) &= \frac{\beta_{e,r}(\Delta h) + 1}{\beta_{e,r}(\Delta h) + \alpha_{e,r}(\Delta h) + 2} \times \lambda_1 \times \lambda_2, \\ \lambda_1 &= \frac{1}{1 + \sqrt{\alpha_{e,r}(\Delta h)/\beta_{e,r}(\Delta h) + \alpha_{e,r}(\Delta h) + 1}}, \\ \lambda_2 &= 1 - \frac{1}{\beta_{e,r}(\Delta h) + \omega}, \end{aligned} \quad (9)$$

where λ_1 is the penalty (i.e., increase of trust loss) against unsuccessful collaboration; λ_2 is the long-term gradual accumulation of the direct trust between two terminals and is used to control the growth rate of $GS_{e,r}(\Delta h)$.

The feedback difference between terminals not involved in collaboration is needed to realize accurate trust matching of the collaboration between HMUTs. The most reasonable calculation basis is the historical feedback the most similar to the current collaboration form. This paper adopts k-means clustering (KMC) to process the historical feedbacks, before selecting the HMUTs based on collaboration similarity.

There are various types of user terminals and diverse forms of collaboration. As a result, there must be some differences in the collaboration form between terminals, even if the terminals are of similar performance and functions. In this paper, the KMC is adopted to initialize a fixed centroid and a random centroid and complete the preliminary filtering based on task similarity. Out of the two clusters obtained through classification, the cluster containing the current collaboration was determined, and all the feedbacks on the cluster were saved. Then, the set of direct trusts can be calculated by

$$GS_{M \rightarrow r}(\Delta h) = \{GS_{1,r}(\Delta h), GS_{2,r}(\Delta h) \dots GS_{n,r}(\Delta h) \dots GS_{m,r}(\Delta h)\}. \quad (10)$$

After the end of the iteration, the KMC divided the feedback set of the object into a large cluster and a small cluster. The mainstream feedbacks from the large cluster were retained, while the abnormal feedbacks from the small cluster were discarded. In this way, the malicious feedbacks were filtered out.

In the above algorithm, the indirect trust obtained from multisource feedbacks is defined as the mean of the feedbacks in the large cluster and helps to compute $OS_{M \rightarrow m}$.

This paper calculates the trust of HMUTs from two perspectives: the state of collaboration and information resources of user terminals, and the historical records. Hence, the composite trust of the system should comprehensively reflect the situation in the two perspectives. To maximize the safety of system management and minimize system risks, this paper carries out the weighted summation of CT value $SU_{e,r}$, direct trust $GS_{e,r}(\Delta h)$, and indirect trust $OS_{M \rightarrow m}$. Based on single dimensional trusts, the composite trust can be solved by

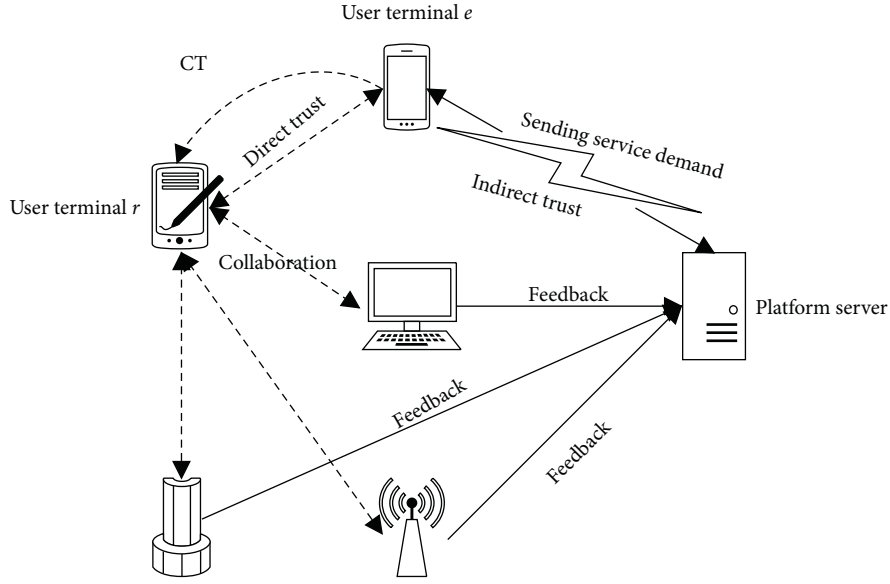


FIGURE 2: Flow of trusted computing of user terminals.

$$QS_{M \rightarrow r}(\Delta h) = \min\{(\theta \times GS_{e,r}(\Delta h) + (1 - \theta) \times OS_{M \rightarrow r}(\Delta h))SU_{e,r}\}. \quad (11)$$

$$\psi_s(q) = \frac{\sum_{d=1}^{|U(q)|} H(d, q)}{|U(q)|} \times D_h(q, h_0, h). \quad (12)$$

3. Trust Management of HMUTs

Figure 3 shows the trust model framework of health monitoring platform. It can be observed that the safety of platform management is largely covered by identity management, authentication, and data protection of users. The safety level of user terminal management must be calculated objectively and truthfully. The overall trust of the system is inseparable from the authentication of user terminals. If the credibility of terminal feedbacks is measured by identity management, the privacy of users might be exposed. To prevent the problem, user information should be processed by password encryption or anonymity technology. However, the current technical level cannot guarantee system efficiency and privacy protection at the same time.

To protect the information privacy of user terminals, the safety management framework needs to be established based on trust. Figure 4 presents the safety management framework of HMUTs. There are three layers in the framework, namely, a safety management service provision layer, a trust management service layer, and a safety management service user terminal layer, which respectively provide users with information safety management, trusted computing, and safety management.

Our trust management service can manage the trusts of multiple HMUTs. The trust refers to the trust evaluation computed from feedbacks of user terminals, after safety management. Let $U(q)$ be all the trust feedbacks on system safety management service q ; $|U(q)|$ be the total number of trust feedbacks; $H(d, q)$ be the trust feedback from user terminal d (its value varies with the d values); $D_h(q, h_0, h)$ be the change rate of trust in a period. Then, the trust evaluation result can be calculated by

To detect whether collusion feedback is used in the safety management service adopted by user terminals, this paper introduces the feedback density to evaluate the reliability of the trust feedbacks from user terminals. Let q be the safety management service for user terminals; $N(q)$ be the total number of feedbacks from user terminals to q . Then, the feedback density $TH(q)$ can be expressed as

$$TH(q) = \frac{N(q)}{|U(q)| \times K(q)}. \quad (13)$$

Let $p_u(q)$ be the threshold of collusion feedback; $|U_d(d, q)|$ be the number of feedbacks submitted by user terminal d to q . Then, the collusion feedback factor $K(q)$ can be calculated by

$$K(q) = 1 + \left(\sum_{g \in U(q)} \left(\sum_{d=1}^{|U_d(d, q)|} \frac{\sum_{|U_d(d, q)| > p_u(q)} |U_d(d, q)|}{|U_d(d, q)|} \right) \right). \quad (14)$$

In a fixed period, the intermittent collision feedback to safety management service q can be defined as the intermittent collision feedback of q and used to characterize the mutation in the feedbacks of user terminals. Let $|U(q)|$ be the total number of trust feedbacks to q in a fixed period $[h_0, h]$; U^* be the preset feedback threshold. Then, we have

$$\frac{|U(q)' - |U(q)|}{|h - h_0|} \times K(q) > U^*. \quad (15)$$

If formula (15) is satisfied, it is highly possible that intermittent collision feedback has occurred. In other words, intermittent collision feedback will occur when the variation of the total trust feedbacks $|U(q)|$ to q in $[h_0, h]$ surpasses a certain level.

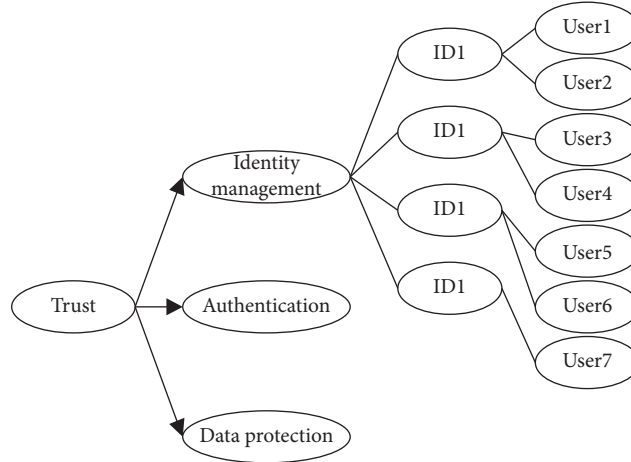


FIGURE 3: Trust model framework of health monitoring platform.

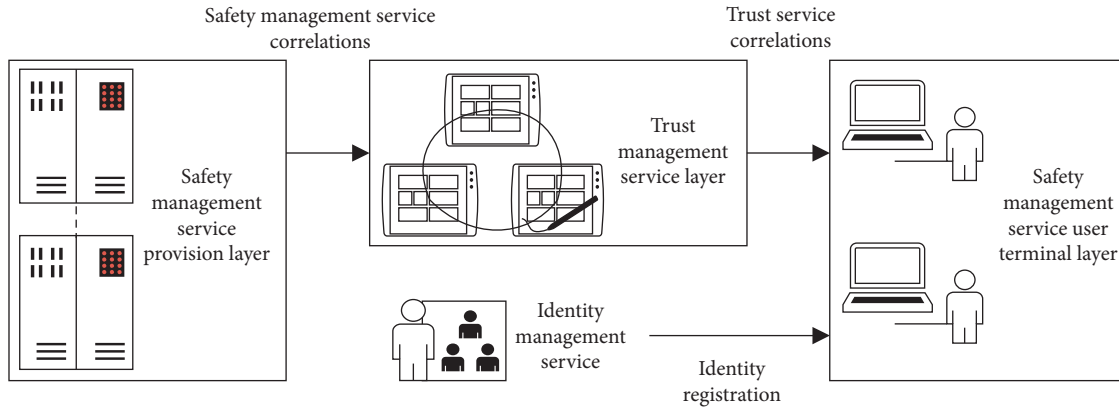


FIGURE 4: Safety management framework of HMUTs.

To enhance the robustness of HMUT trusted computing model against malicious attacks, this paper first computes the trust of user terminals to exclude some malicious users, thereby mitigating the threat to safety management service. Let $B_{d_i \rightarrow q_j}^{h_l}$ be the service provision capability of safety management service q_j received by user terminal d_i at time h_l ; h_l be the time of the l -th transaction. Then, we have

$$B_{d_i \rightarrow q_j}^{h_l} = \left\{ B_{d_i \rightarrow q_j, Nf_1}^{h_l}, \dots, B_{d_i \rightarrow q_j, Nf_w}^{h_l} \right\}, \quad (16)$$

where $0 < B_{d_i \rightarrow q_j, Nf_1}^{h_l}, \dots, B_{d_i \rightarrow q_j, Nf_w}^{h_l} \leq 1$ is the service provision capability of the h -th index Nf_h ($1 \leq h \leq w$) of $B_{d_i \rightarrow q_j}^{h_l}$.

The user terminal satisfaction with safety management was defined as the difference between the actual service capability provided by safety management service q_j to user terminal d_i and the service capability to be realized by q_j . The satisfaction $\sigma(d_i, q_j, h_l)$ of d_i with safety management service provided by q_j at time h_l can be calculated by

$$\sigma(d_i, q_j, h_l) = \sum_{h=1}^w \xi_{d_i \rightarrow q_j, Nf_h}^{h_l}. \quad (17)$$

Let $0 < B_{q_j, Nf_w}^{h_l} \leq 1$ be the service capability to be realized by q_j at time h_l corresponding to the h -th index Nf_h . Then,

the index $\xi_{q_j, Nf_h}^{h_l}$ of safety management service capability in formula (17) can be calculated by

$$\xi_{d_i \rightarrow q_j, Nf_h}^{h_l} = \begin{cases} 1, & B_{d_i \rightarrow q_j, Nf_h}^{h_l} - B_{q_j, Nf_h}^{h_l} \geq 0, \\ v \left| B_{d_i \rightarrow q_j, Nf_h}^{h_l} - B_{q_j, Nf_h}^{h_l} \right|, & B_{d_i \rightarrow q_j, Nf_h}^{h_l} - B_{q_j, Nf_h}^{h_l} < 0. \end{cases} \quad (18)$$

If $B_{d_i \rightarrow q_j, Nf_h}^{h_l} - B_{q_j, Nf_h}^{h_l} \geq 0$, $B_{q_j, Nf_h}^{h_l}$ satisfies the demand of user terminal d_i , and the satisfaction of Nf_h with safety management service is 1. If $B_{d_i \rightarrow q_j, Nf_h}^{h_l} - B_{q_j, Nf_h}^{h_l} < 0$, $B_{q_j, Nf_h}^{h_l}$ deviates from the demand of user terminal d_i ; since $0 < v < 1$, the greater the deviation, the smaller the value of $\xi_{q_j, Nf_h}^{h_l}$, that is, the less the user terminal's satisfaction with the safety management service.

To compute composite trust in time, this paper computes the trust of user terminal d_i in safety management service q_j within a time window TW . The trust can be derived from the satisfaction of d_i with each service q_j within the time window. Let h_f be the current time, $c = \min\{l | h_l \in TW\}$; $v(l) = t^{h_f - h_l}$ be the time attenuation function, $0 < t < 1$; $g = f - c$ be the number of services received by user terminal d_i within TW ; $\Psi(g) = e^{-1/g}$ be the number of safety management services. Then, we have

$$\Phi_{d_i, q_j}^{h_f} = \frac{\Psi(g) \sum_{l=c}^f v(l) \sigma(d_i, q_j, h_l)}{\sum_{l=c}^f v(l)}. \quad (19)$$

Formula 19 shows the more the number of safety management services in TW , the greater the $\Psi(g)$, the larger the $\Phi_{d_i, q_j}^{h_f}$, the more trustworthy the safety management services.

The credibility characterizes the actual performance of a safety management service. The users can choose to accept or reject a safety management service according to the level of credibility. If the credibility of safety management services is too low, the health monitoring platform will face the risk of losing users. Let $D = (d_1, \dots, d_m)$ be the set of users receiving safety management service q_j within TW ; $|D|$ be the number of user terminals receiving safety management service q_j within that time window. Then, the credibility $CR_{q_j}^{h_f}$ of q_j perceived by user terminal d_i within TW can be calculated by

$$CR_{q_j}^{h_f} = \frac{\sum_{i=1}^m \Phi_{d_i, q_j}^{h_f}}{|D|}, \quad (20)$$

where $\mu \in (0, 1)$ is a preset parameter. Formula 20 shows that the more user terminals receiving q_j within TW , the greater the $1/\mu^{|D|}$, the higher the credibility of q_j .

In this paper, the satisfaction of d_i with q_j is characterized by the difference $DS_{q_j, d_i}^{h_f}$ between the credibility $CR_{q_j}^{h_f}$ of safety management service q_j and the credibility $\Phi_{d_i, q_j}^{h_f}$ of q_j perceived by user terminal d_i . Let $CR_{d_i, q_j}^{h_f}$ be the credibility of q_j at the latest update. Then, we have

$$DS_{q_j, d_i}^{h_f} = \begin{cases} \alpha \left| \Phi_{q_j, d_i}^{h_f} - F_{q_j}^{h_f-1} \right|, & \left| \Phi_{q_j, d_i}^{h_f} - CR_{q_j}^{h_f-1} \right| \leq \omega, \\ -\alpha \left| \Phi_{q_j, d_i}^{h_f} - F_{q_j}^{h_f-1} \right|, & \left| \Phi_{q_j, d_i}^{h_f} - CR_{q_j}^{h_f-1} \right| > \omega. \end{cases} \quad (21)$$

where ω is a preset threshold; $\alpha \in (0, 1)$ is a preset parameter. If $|\Phi_{d_i, q_j}^{h_f} - \Phi_{d_i, q_j}^{h_f-1}| \leq \omega$, the credibility of safety management service q_j perceived by user terminal d_i is not very different from the credibility of q_j . In this case, the user terminal makes a relatively objective evaluation of the safety management service. The smaller the difference, that is, the greater the $DS_{q_j, d_i}^{h_f}$, the more objective the evaluation. If $|\Phi_{d_i, q_j}^{h_f} - \Phi_{d_i, q_j}^{h_f-1}| > \omega$, the user terminal fails to make an objective evaluation of the safety management service.

4. Experiments and Results Analysis

To verify its feasibility, our model (model 1) was compared with four other models: the trusted computing model coupling similarity and information entropy (model 2), multisource feedback trusted computing model (model 3), trusted computing model based on improved Dempster-Shafer (D-S) evidence theory (model 4), and lightweight trusted computing model (model 5).

During the experiment, the proportion of low-competence terminals on the platform was gradually increased from 0% to 60% to simulate the influence of different trusted

computing models on the success rate of collaboration between user terminals, as the number of low-competence terminals gradually increases in real working. Figure 5 presents the variation in the success rate of collaboration between user terminals with the proportions of low-competence terminals derived by each model. The term low-competence terminal refers to the user terminal, whose information resources cannot match demand because its utilization of information resources changes too rapidly.

As shown in Figure 5, with the growing proportion of low-competence terminals, the success rate of collaboration of models 1–3 changed stably, while that of model 4 and model 5 declined more and more steeply. This is because our model can evaluate the capability of user terminals based on the current state of information resources and suppress the risk of safety management failure induced by terminal collaboration. To sum up, the experimental results demonstrate that our model can effectively handle the variation in the number of low-competence terminals and the situation of information resources and achieve good robustness.

Based on the in-depth understanding of the nature and features of attacks, scholars have constructed various attack models, such as attack tree, attack network, attack graph. Figure 6 provides our attack model, where the abscissa is the time node, and the ordinate is the number of feedbacks from user terminals.

To verify the overall effect of the safety management system for HMUTs against malicious terminals, this paper tests the success rate of collaboration at different proportions of malicious terminals. During the experiment, the proportion of malicious terminals was gradually increased from 0% to 60%.

Figure 7 presents the relationship between the proportion of malicious terminals and the success rate of collaboration, as derived by each model. It can be observed that all models had a high success rate of collaboration when malicious terminals took up a small proportion. After the proportion increased to a high level, the models differed in terms of the success rate of collaboration. Our trusted computing model performed better than the other models, in the presence of the same malicious attacks.

Considering the low delay requirement of safety management systems, this paper measures the complexity of the proposed trusted computing mechanism and tries to improve the multidimensional trusted computing model for HMUTs. Two core metrics were selected to evaluate model performance: the time cost and robustness of function execution. As shown in Figure 8, our model converged within less time than the other models, reflecting the excellence of our model in a lightweight design.

The above three experiments demonstrate that our trusted computing model is lightweight, accurate, reliable, and stable.

Next, the authors further verified the effectiveness of our trust-based safety management scheme. Figure 9 provides the trust measured by our model and that measured by model 2, which performs similarly with our model. The blue line is the trust measured by the reference model 2, while the dashed line is the trust measured by our model. Figure 10 compares the precision and recall of the two models.

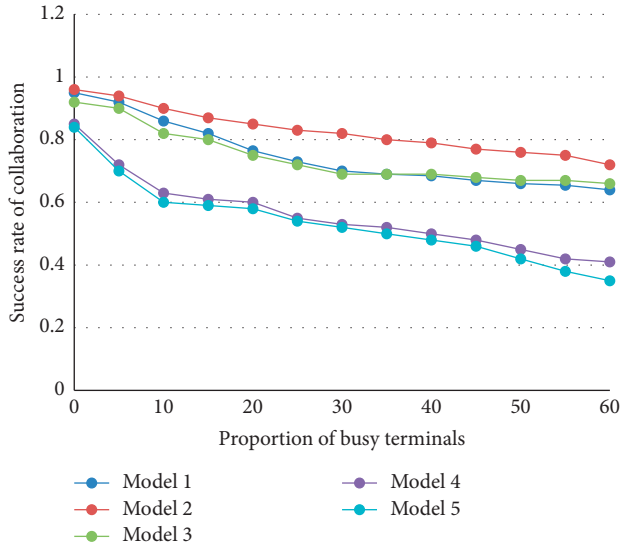


FIGURE 5: Relationship between the proportion of low CT terminals and success rate of collaboration.

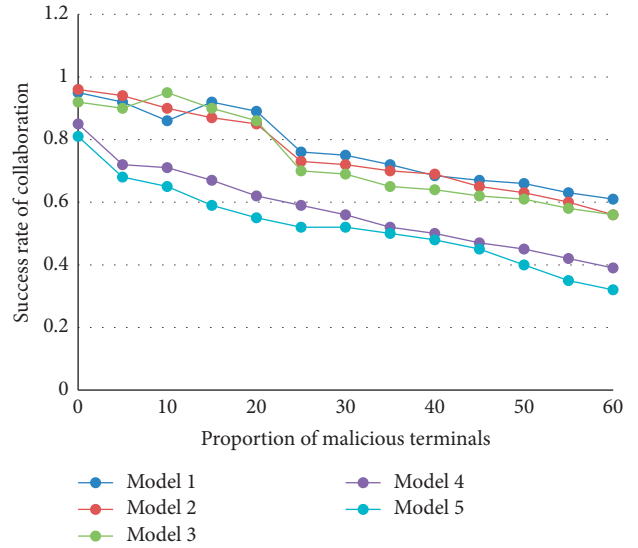


FIGURE 7: Relationship between the proportion of malicious terminals and success rate of collaboration.

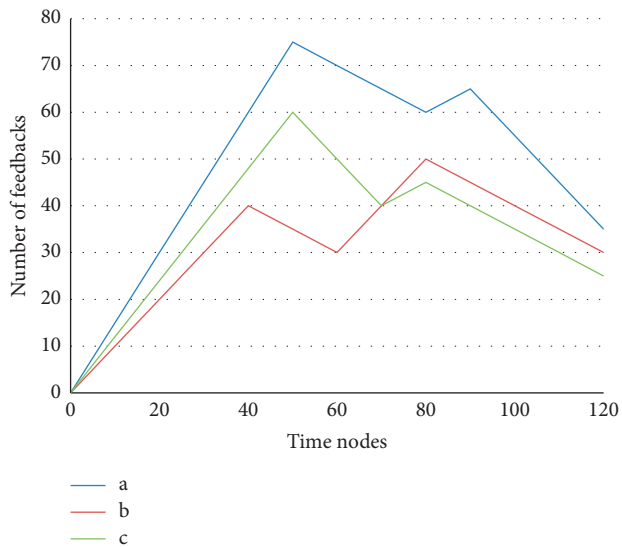


FIGURE 6: Attack model.

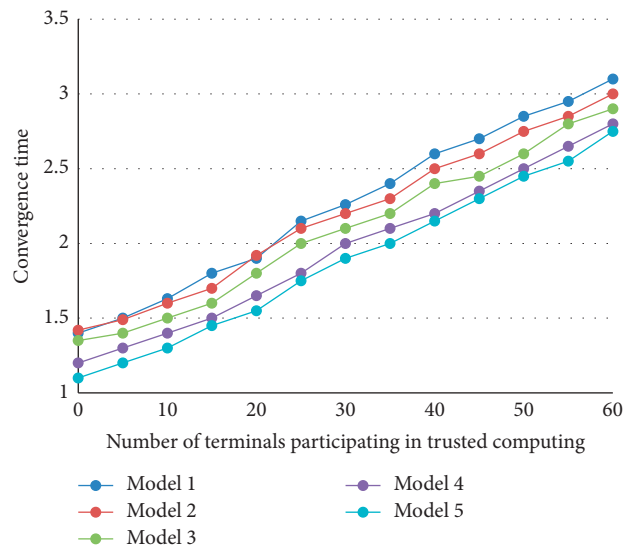


FIGURE 8: Convergence time of different models.

When the credibility was computed by the reference model, the trust was high at 10s, because the numerous malicious feedbacks submitted by malicious users exaggerate the trust of the safety management services. When our trust-based model was adopted for computing, the trust value fluctuated very slightly. The fluctuation (<0.05) was so small as to be negligible. This confirms that our model can effectively resist the collusion attacks by malicious users. In addition, the high recall of our model indicates that the proposed model can correctly judge whether a safety management service is under collusion attack.

The precision was obtained by comparing the trust of a safety management service with the trust promised by the

platform, while the recall was calculated by comparing that with the trust perceived by user terminals.

Figure 11 presents the precisions and recalls of our model (blue curves) and reference model (red curves). It is obvious that the precisions and recalls of both models decreased slightly with the growing number of safety management services. The reason is that the increase of such services adds difficulty to model computing and increases the computing error. Of course, our model performed better than the reference model and achieved higher precision and recall. In summary, our model is an ideal tool to compute the safety level of safety management services.

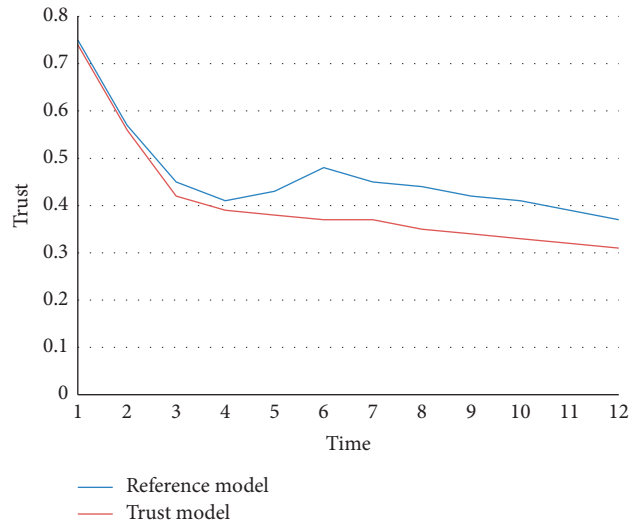


FIGURE 9: Measured trust.

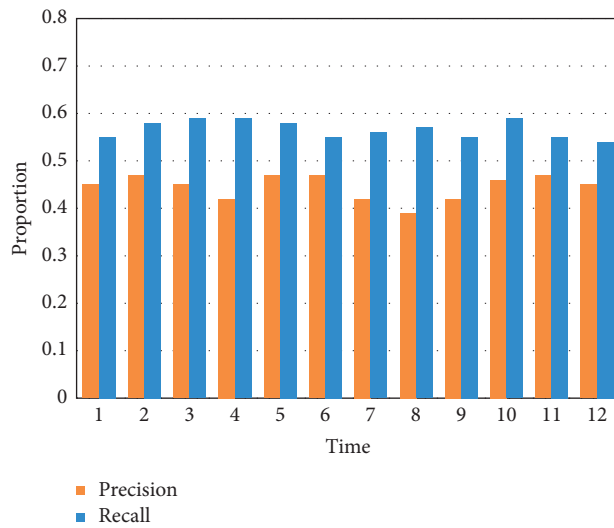


FIGURE 10: Measured precision and recall.

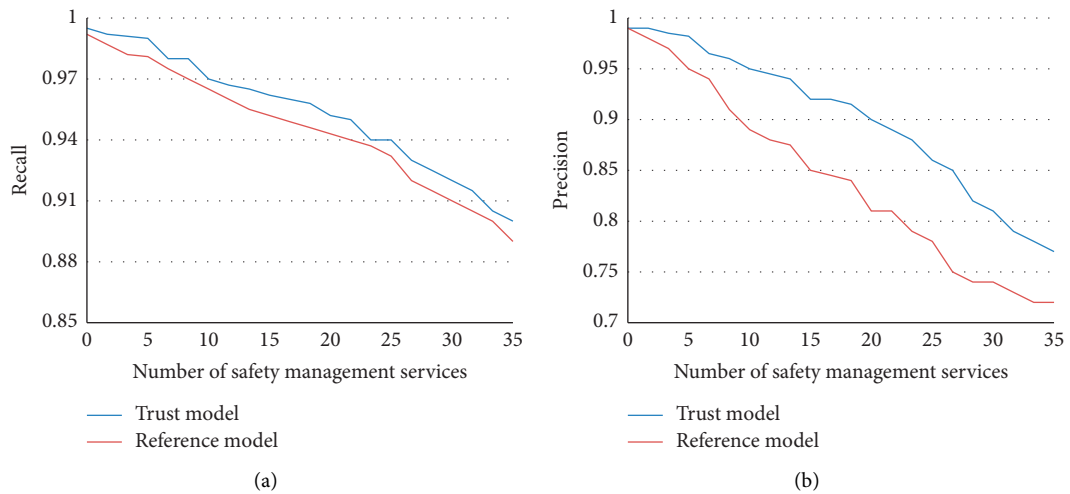


FIGURE 11: Precisions and recalls of our model and reference model.

5. Conclusions

This paper investigates the safety management solution for HMUTs based on trusted computing. First, the authors set up a multidimensional trusted computing model for HMUTs. Then, the computing method was detailed for composite trust based on single-dimensional trust. After that, a trust management scheme was prepared for HMUTs.

The proposed model was compared experimentally with four other models. Specifically, the authors plotted the relationship between the success rate of collaboration and the proportion of low-competence terminals and that between the success rate of collaboration and the proportion of malicious terminals. The relationship curves confirm that our trusted computing model outperformed the other models in resisting the same malicious attacks. Furthermore, the trust, precision, and recall of our model were contrasted with a reference model. The comparison demonstrates that our model performed better than the reference model and achieved higher precision and recall.

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.

References

- [1] S. Phaltankar, K. Tyagi, M. Prabhu, P. Jaguste, S. Sahu, and D. Kalbande, "CuraBand: Health monitoring and warning system," in *Proceedings of the International Conference on Innovative Computing and Communications*, pp. 1017–1026, Springer, Singapore, 2021.
- [2] C. E. Gillies, D. F. Taylor, B. C. Cummings et al., "Demonstrating the consequences of learning missingness patterns in early warning systems for preventative health care: A novel simulation and solution," *Journal of Biomedical Informatics*, vol. 110, Article ID 103528, 2020.
- [3] K. L. Walkup, "Disrupting dominant narratives: Mental health, early warning systems, and threat construction," in *Proceedings of the 38th ACM International Conference on Design of Communication*, pp. 1–2, New York, NY, USA, 2020.
- [4] M. Morabito, A. Messeri, A. Crisci, L. Pratali, M. Bonafede, and A. Marinaccio, "Heat warning and public and workers' health at the time of COVID-19 pandemic," *The Science of the Total Environment*, vol. 738, Article ID 140347, 2020.
- [5] M. Gustin, R. S. McLeod, K. J. Lomas, G. Petrou, and A. Mavrogianni, "A high-resolution indoor heat-health warning system for dwellings," *Building and Environment*, vol. 168, p. 106519, 2020.
- [6] S. McElroy, L. Schwarz, H. Green et al., "Defining heat waves and extreme heat events using sub-regional meteorological data to maximize benefits of early warning systems to population health," *The Science of the Total Environment*, vol. 721, p. 137678, 2020.
- [7] S. Nandy and M. Adhikari, "Intelligent health monitoring system for detection of symptomatic/asymptomatic COVID-19 patient," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20504–20511, 2021.
- [8] S. Mousavi, D. B. Kara, and S. S. Seker, "Integrated fault evaluation through fusion algorithm supported by Kalman filter," *Traitement du Signal*, vol. 37, no. 6, pp. 975–987, 2020.
- [9] M. Malathi, S. Pavithra, S. Preakshanashree, and S. P. Kumar, "Intelligent driving detection with health monitoring and accident detection system using IOT," *Journal of Physics: Conference Series*, vol. 1916, no. 1, p. 012036, 2021.
- [10] A. Rahaman, M. Islam, M. Islam, M. Sadi, and S. Nooruddin, "Developing IoT based smart health monitoring systems: A review," *Revue d'Intelligence Artificielle*, vol. 33, no. 6, pp. 435–440, 2019.
- [11] J. Elouni, H. Ellouzi, H. Ltifi, and M. B. Ayed, "Intelligent health monitoring system modeling based on machine learning and agent technology," *Multiagent and Grid Systems*, vol. 16, no. 2, pp. 207–226, 2020.
- [12] T. J. Swamy and T. N. Murthy, "eSmart: An iot based intelligent health monitoring and management system for mankind," in *Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–5, IEEE, Coimbatore, India, Jan. 2019.
- [13] J. Vogel and A. Kelkar, "Aircraft control augmentation and health monitoring using flush air data system feedback," in *Proceedings of the 26th AIAA applied aerodynamics conference*, Honolulu, HI, USA, 2008.
- [14] D. Gartenberg, R. Thornton, M. Masood, D. Pfannenstiel, D. Taylor, and R. Parasuraman, "Collecting health-related data on the smart phone: Mental models, cost of collection, and perceived benefit of feedback," *Personal and Ubiquitous Computing*, vol. 17, no. 3, pp. 561–570, 2013.
- [15] A. Gupta, C. Chakraborty, and B. Gupta, "Monitoring of epileptical patients using cloud-enabled health-IoT system," *Traitement du Signal*, vol. 36, no. 5, pp. 425–431, 2019.
- [16] L. Xie, F. Hang, Y. Lv, and W. Guo, "Research on data security protection system of monitoring and acquisition system based on block chain technology," *Advances in Artificial Intelligence and Security, Communications in Computer and Information Science*, pp. 502–513, 2021.
- [17] W. Tao, J. Wu, Z. Liang, and Z. Jiang, "Trusted security immune model of power monitoring system," *Journal of Physics: Conference Series*, vol. 1744, no. 2, p. 022115, 2021.
- [18] G. Wu, "Monitoring system of key technical features of male tennis players based on internet of things security technology," *Wireless Communications and Mobile Computing*, vol. 2021, p. 4076863, 2021.
- [19] V. Narayana, A. Gopi, and K. Chaitanya, "Avoiding interoperability and delay in healthcare monitoring system using block chain technology," *Revue d'Intelligence Artificielle*, vol. 33, no. 1, pp. 45–48, 2019.
- [20] B. Dai, "Research on security monitoring system for wind-solar complementary power generation based on internet of things," *International Journal of Information and Communication Technology*, vol. 17, no. 1, pp. 91–106, 2020.
- [21] A. Kamble and S. Bhutad, "Iot based patient health monitoring system with nested cloud security," in *Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA)*, pp. 1–5, IEEE, Greater Noida, India, Dec. 2018.
- [22] A. Ray and H. Ray, "Wearable sensors based smart secured remote health monitoring system," in *Proceedings of the 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, pp. 1–6, IEEE, Bhilai, India, Feb. 2021.

- [23] Y. E. Jiang and J. Liu, "Health monitoring system for nursing homes with lightweight security and privacy protection," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–11, 2017.
- [24] M. Ahmid, O. Kazar, S. Benharzallah, L. Kahloul, and A. Merizig, "An intelligent and secure health monitoring system based on agent," in *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 291–296, IEEE, Doha, Qatar, Feb. 2020.
- [25] R. Kesavan and S. Arumugam, "Adaptive deep convolutional neural network-based secure integration of fog to cloud supported Internet of Things for health monitoring system," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 10, p. e4104, 2020.
- [26] H. Somaya and M. Tomadar, "Secure communication in E-health care system monitoring," in *Proceedings of the 4th International Conference on Smart City Applications*, pp. 1–9, New York, NY, USA, 2019.
- [27] T. Wearing and N. Dragoni, "Security and privacy issues in health monitoring systems: eCare@Home case study," in *Proceedings of the International Conference on IoT Technologies for HealthCare*, pp. 165–170, Porto, Portugal, February 2017.