International Journal of Web Services Research
Volume 21 • Issue 1

Application of Internet of Things Technology in Computer Network Security and Remote-Control Analysis

Shouning Huang, Guangxi Technological College of Machinery and Electricity, China*

ABSTRACT

Internet of things computer network technology can not only speed up the information transmission, but also help to break the previous time and space restrictions and improve the actual work efficiency. However, in the practical application and development of this technology, the realization of data security technology and remote control technology is the key to improve its application effect and ensure data security. Due to the obvious openness of the internet of things computer network itself, common security risks emerge one after another. Therefore, in practical application, it is necessary to pay more attention to security management and maintain network security.

KEYWORDS

Computer, Internet of Things Technology, Network Security, Remote Control

INTRODUCTION

With the increasing level of computer network applications, the factors affecting computer network security are also increasing. Various network crises such as personal privacy exposure, network virus invasion, system vulnerability, hacking and other serious threats have become a great concern in the world (Aggarwal et al., 2020). The Internet of Things (IoT), as the third wave of the world's information industry after computers and the Internet (Aldaej, 2019), has also made rapid progress against the backdrop of the growing technological level in China.

IoT technology enables the establishment of interconnected channels among objects via networks. In terms of its components, IoT is characterized by a layered structure that distinguishes different functionalities. For instance, the application layer is responsible for processing relevant data and information, as well as making final decisions based on them. (Al-Sibai et al., 2021). The network perception layer needs to acquire the state of objects according to the tasks corresponding to its own operational functions, and the tasks of the information network layer need to transmit information in an orderly manner and collect the corresponding data. IoT technology and remote-control technology are integrated into the IoT smart home, and wireless technology is used to speed up the transmission of information. The IoT serves as a carrier for basic data connectivity and realizes the mutual integration

DOI: 10.4018/IJWSR.342120 *Corresponding Author

between things and networks. Through remote control technology, the internet is used to effectively control remote devices and ensure the secure operation of computer networks. However, as IoT devices continue to expand, network security issues become more complex and critical. Securing the IoT, especially in terms of data transmission and device authentication, becomes particularly important (Sitaraman, 2022). In response to these challenges, further research and development of secure and reliable routing mechanisms, device authentication mechanisms, and the like are needed to ensure the security and stability of IoT systems (Chatfield & Reddick, 2019).

The rapid development of the IoT brings great convenience to people's lives and privacy issues. Therefore, it becomes crucial to construct a secure and reliable privacy protection mechanism (Dovhan et al., 2019).

The objective of this thesis is to explore the development of a resilient privacy protection mechanism within the IoT technology environment. The study begins by examining the utilization of digital signature techniques for encrypting network data, thereby ensuring its confidentiality and integrity. Additionally, focus is placed on employing various security techniques, including encryption, firewalls, intrusion detection, and prevention systems, to safeguard network security against the growing sophistication of cyber threats.

In the IoT environment, we further explore the design and implementation of secure routing mechanisms. By rationally planning the network topology, optimizing routing algorithms and introducing fault recovery mechanisms, we aim to improve the robustness and reliability of IoT systems.

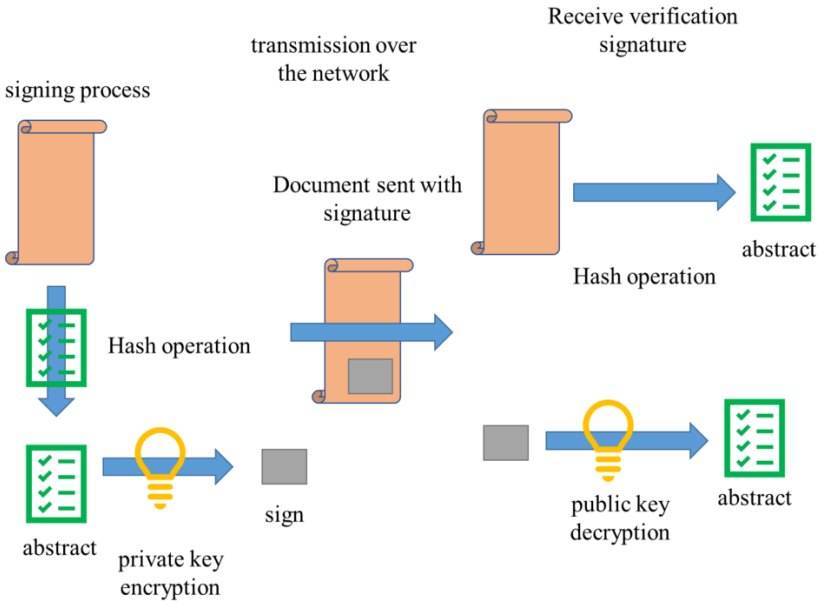
In addition, we will study techniques in authentication and remote control to ensure that only authorized users can access and operate IoT devices.

By conducting detailed validation experiments and performance analysis, the feasibility and effectiveness of the proposed mechanisms will be evaluated. The research aims to offer substantial evidence supporting the construction of a secure and reliable privacy protection mechanism, thereby fostering the sustainable development of IoT technology.

RELATED WORKS

Li (2013) presents the implementation details of the protocol. As people pay more attention to the security of network communication, in order to improve the security of computer network communication, the application of data encryption technology has become an important technical means (Li, 2013). Based on Zhang (2018), we make an in-depth analysis on the application of data encryption technology in computer network communication security. With the expansion of the current application of big data technology, the application in computer network information security has gradually developed, which has a positive effect on improving computer network information security and protection benefits. Chu et al. (2021) conduct analysis of network security and privacy security based on AI in the IoT environment. The network security risks caused by AI and IoT applications are analyzed in Chu study. In the application of computer network communication security technology, the application of data encryption technology is to ensure people's privacy and security. Chen makes a preliminary analysis and discussion on the problems of computer network management and information security prevention (2021). Data is the basis of information technology security management, and with the arrival of the era of big data, computer network security also faces many challenges. The network has open and virtual characteristics, which present many security risks (He, 2021). He (2021) explores the main hidden network security danger and puts forward the corresponding precautions to the computer information network security precautions. The information age Internet technology is widely used, but computer network security problems also often appear, often a variety of viruses invade the computer, so He strengthen the network security management, and put forward countermeasures, so as to improve the level of network security, strengthen network security protection, is very important (He, 2021) .

Figure 1. Realization flowchart of digital signature technology



Based on the literature review, it can be seen that previous research has mainly focused on the application of data encryption technology in computer network communication security, the application of big data technology in network information security, and the analysis of network security and privacy security based on AI in an IoT environment. Addressing the gaps in the research area, this thesis proposes secure and reliable routing mechanisms and device authentication mechanisms to deal with security and privacy issues in the Internet of Things. These mechanisms may help to secure communications, prevent information leakage and unauthorized access, and provide effective network management and privacy protection.

IoT Computer Network Security and the Optimization Path of Remote-Control Technology

Stable and Reliable Privacy Protection Mechanism

In order to maximize its value and effect in practice, a stable and reliable privacy protection mechanism should be constructed during the implementation of the technology. This will not only enable the data transmission process to have strong stability, but will also help reduce the probability of security problems and implement an integrated work idea so as to identify the right direction for follow-up work (Isravel et al., 2018). Implementing a robust and dependable privacy protection method helps to minimize the probability of security issues by protecting sensitive data against prohibited access and disclosure, improving user confidence, maintaining regulatory compliance, and protecting against cyber threats (Heriadi & Pamuji, 2020).

Figure 1 shows the most important data encryption technology in privacy protection. This technology mainly encrypts the network data that needs to be transmitted and shared by means of the form of encryption function transformation or the form of secret key. After these data are encrypted, they need to be recovered by means of a function decryption method or decryption key, and then presented in plaintext to ensure communication security (Wu et al., 2021).

When building a stable and reliable privacy protection mechanism, it is necessary to strengthen the in-depth analysis of the characteristics of the entire information link channel and integrate

advanced technical solutions, so that the establishment of the privacy protection mechanism can be comprehensively improved (Alkali et al., 2022). The technical model focuses on maintaining the security of the network technology itself, properly integrating various technologies and continuously optimizing the current technical solutions to support the subsequent privacy protection mechanism. To ensure network security, the technical model involves integrating different technologies, including encryption, firewalls, and intrusion detection and prevention systems, among others, to provide a comprehensive defense against various cyber threats (Javed et al., 2022).

The privacy protection mechanism mainly needs to establish a hierarchical work system, starting from the management aspect, and integrate into a reasonable interconnection. A hierarchical work system can be effective for privacy protection by ensuring clear roles and responsibilities, access controls, employee training and awareness, regular monitoring and auditing, and a clear incident response plan for dealing with breaches (Kashiyama et al., 2021). Network equipment and corresponding information protection codes are enhanced to strengthen the management of data information, thereby providing an important security protection barrier for personal information settings (Yilmaz & Uludag, 2021). In addition, through technical authorization and technical certification, the security factor of terminal equipment can be comprehensively improved, and at the same time, it must play an absolute defense against external attacks, and continuously optimize the current technical system, so that the overall communication effect can be comprehensively improved (Alkali et al., 2022). When the actual system is established, the data and information must be transmitted through the supervisory control and data acquisition (SCADA) system of the human-computer interaction control device, and the corresponding control authority must be password protected to prevent intrusion.

Because of the network's complex characteristics, the corresponding tasks are also quite complex, resulting in frequent network security problems. Therefore, in the actual implementation, it is necessary to manage the application of wireless sensor network nodes through network communication security, according to the characteristics of different nodes (Tzafestas, 2012). Wireless sensor network (WSN) nodes are crucial for collecting and communicating data in various applications. Ensuring network communication security is essential to protect the privacy and integrity of the transmitted data. WSN nodes can use techniques such as encryption, secure communication protocols, intrusion detection, physical security, and authentication to enhance network security (Thota et al., 2023). It is important to establish a security management protocol to reduce the probability of malicious attacks and illegal intrusions from the outside world. Security management protocols employ various strategies to minimize the likelihood of malicious attacks and illegal intrusions. These include risk assessment, access control, network security, incident response planning, system updates, employee training, and physical security measures. Regular review and updating of these measures are necessary to stay ahead of evolving threats (Kimani et al., 2019). In the implementation of technology, it is necessary to match the characteristics of the Internet of Things network to further optimize the operating environment of network communication. Mechanisms such as transmission of data packets and keys can be adopted to provide important guarantees for network security management (Matey Akwetey et al., 2022).

MATERIALS AND METHODS

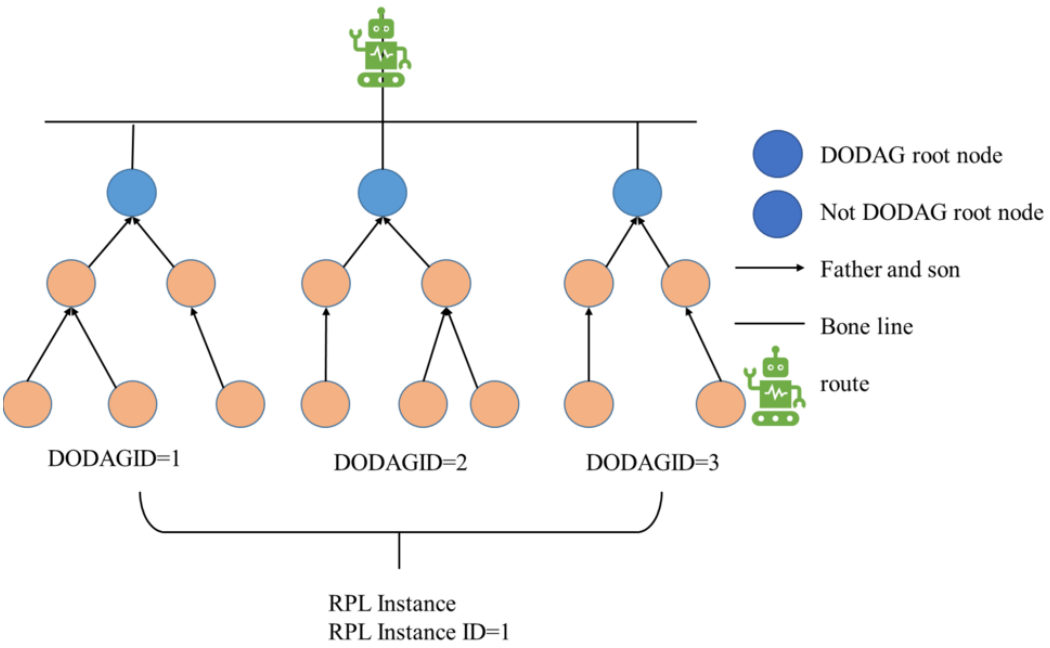
Industries with IoT-centric concepts are now ubiquitous. In computer network security and technology, with the increasing number of heterogeneous devices, the IoT is more likely to be attacked by malicious nodes and suffer greater security threats. Unauthorized access and other aspects have been severely challenged, and the existing resource sharing schemes have given insufficient consideration to privacy protection, security of shared data, and data access control.

Secure Routing Mechanism in the Network Environment of IoT Technology

The IPv4 protocol of the existing IoT environment has problems such as insufficient addresses, mobility, and security. The IPv6-based low-power lossy link network routing mechanism RPL routing protocol is the main improvement method to solve the insufficient address. The IPv4 protocol may handle data packets up to 65,535 bytes in length (including the header and data) and loads up to 65,515 bytes in length. Although IPv4 might provide many distinctive addresses, the increase in internet-connected devices has made it difficult to obtain addresses. This problem was addressed with the development of IPv6, which utilizes 128-bit addresses. Technologies such as mobile IP and IPsec have been developed to solve mobility and security issues. However, security threats remain.

The types of attacks are divided into four categories: trust-based RPL routing security protocol, key authentication-based RPL routing protocol, hierarchical structure-based RPL routing protocol, and specific attack-based RPL routing protocol. The trust-based RPL routing security protocol establishes trust between nodes by assigning trust values based on factors like behavior, communication reliability, and number of neighbors. Nodes with higher trust values are preferred for routing. Then, the key authentication-based RPL routing protocol uses cryptographic keys to authenticate nodes and ensure network security. It distributes unique keys using a hierarchical key management system, with higher-level keys authenticating lower-level ones. Further, the hierarchical structure-based RPL routing protocol organizes nodes into multiple levels within a hierarchical structure. Nodes in higher levels can communicate with lower ones, and a root node manages communication within the network. The specific attack-based RPL routing protocol defends against specific attacks such as sinkhole attacks. It detects and prevents attacks using methods such as hop count limit, energy consumption, and routing path validation. By analyzing node behavior, it can identify and isolate malicious nodes. As shown in Figure 2, the RPL protocol establishes a network topology based on the target-oriented directed acyclic graph DODAG(Destination-Oriented Directed Acyclic Graph). DODAG defines a tree-like structure, but the DODAG structure is not a typical tree, as its nodes may be related to multiple associated with the parent node. It organizes nodes hierarchically, with each node having

Figure 2. RPL example



a parent and potentially multiple children, and the root being the destination node. DODAGs allow for efficient and adaptable routing, as nodes can dynamically adjust their relationships in response to changes in network conditions. This makes RPL valuable for IoT applications.

RPL used to monitor its neighbor's sending behavior, and the local trust value of the neighbor node is obtained; the trust value report is to use the SDN-WISE topology discovery message to carry out the trust value. It is transmitted and uploaded to the controller; the controller implements the isolation response to malicious nodes by calculating and analyzing it and publishing the flow table below.

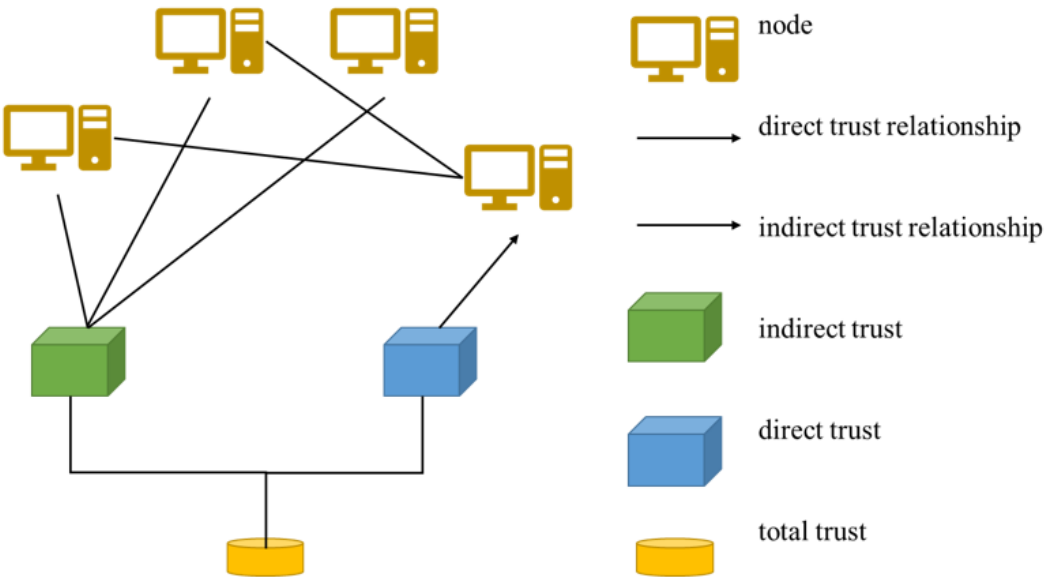
Such a trust value can reflect the level of trust between nodes and the steps it will perform as expected. In this scheme, each node in the RPL network monitors its neighboring nodes to check whether they comply with the specifications of the RPL protocol, or whether they deviate from the specifications of the RPL protocol as shown in Figure 3.

(1) Each node operates in promiscuous mode, so they can eavesdrop on adjacent packet transmissions
(2) Each malicious attack node will start to drop routing packets over time.

Once the node receives the data packet, it sends acknowledgement (ACK) feedback information to the sender.

The node receives the packet success rate. The RPF packet success rate information is obtained by a node through the RPF check on incoming packets, tracking successful and failed RPF-checkable packets. Network administrators can use this information to assess the efficiency of RPF checks in maintaining network security and dependability. Node j is monitored for node i to confirm how many ordinary ACK packets node j has sent, and then the proportion of packets received by node j can be obtained. According to the change of the ratio, it can be known whether node j has malicious behavior. Its success rate is expressed as:

Figure 3. RPL trust mechanism



$$RPF_{i,j}(t) = \frac{RP_{ij}(t) - RP_{ij}(t-1)}{RP_{ij}(t) + RP_{ij}(t-1)} \tag{1}$$

Packet forwarding success rate TPF. Since it is impossible for most nodes to communicate directly with the base station, multiple hops are usually required:

$$TPF_{i,j}(t) = \frac{FP_{ij}(t) - FP_{ij}(t-1)}{FP_{ij}(t) + FP_{ij}(t-1)} \tag{2}$$

When an attack affecting the rank value of nodes occurs in an RPL network, the nodes are actually far away from each other but become neighbors due to the influence of malicious rank values and thus exhibit lower rank values. The rank value monitoring of the node can be expressed as:

$$RKF_{i}(t) = \frac{R_{i}(t)}{R_{i}(t-1)} \tag{3}$$

Package conformance (CPF). Data packets According to the application, the packets sent between adjacent nodes are similar in the same area. The sameness factor is added here to prevent malicious nodes from modifying the main packet:

$$CPF_{i,j}(t) = \frac{EP_{ij}(t)}{EP_{ij}(t) + NEP_{ij}(t)} \tag{4}$$

The direct trust value (DTE) of the node is:

$$DTE_{i,j}(t) = RPF_{i,j}(t) + TPF_{i,j}(t) + RKF_{i,j}(t) + CPF_{i,j}(t) \tag{5}$$

The indirect trust value (ITE) of the node is:

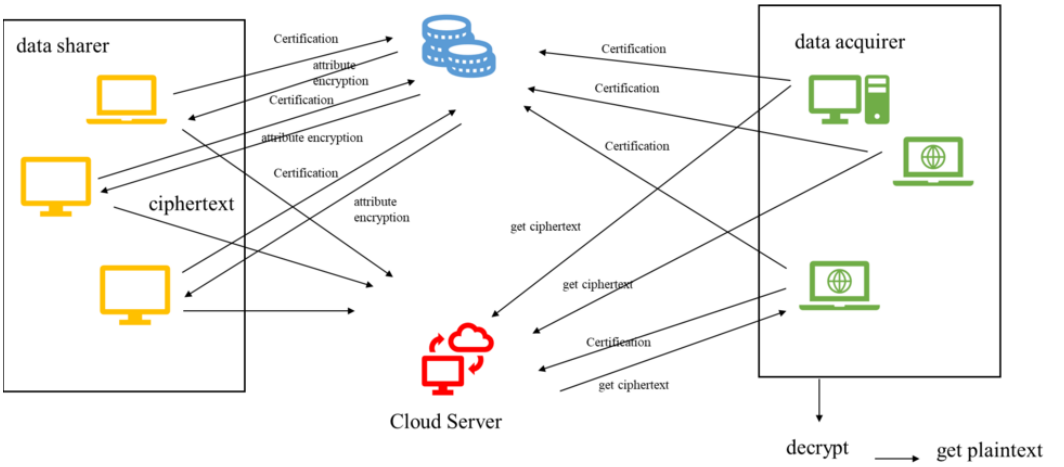
$$ITE_{i,j}(t) = DTE_{i,j}(t) \times DTE_{k,j}(t) \tag{6}$$

The total trust value (TTE) of the node is:

$$TTE_{i,j}(t) = DTE_{i,j}(t) + ITE_{k,j}(t) \tag{7}$$

The perception layer node under the software defined networking solution for wireless sensor networks (SDN-WISE) framework contains three data structures: the WISE state array, the accepted IDs array, and the WISE flow table. SDN-WISE utilizes SDN architecture to manage wireless sensor networks (WSNs). The network topology is defined by the physical layout and communication links between the sensor nodes.

Figure 4. Identity authentication system model based on ciphertext attributes



The SDN controller maintains a global view of the network topology using periodic broadcasts, discovery protocols, and manual configuration. This topology information is vital for network management tasks such as routing, load balancing, and security enforcement, enabling efficient and reliable WSN operation. Uploading the trust value to the SDN controller adopts the topology discovery (TD) protocol proposed by SDN-WISE. The TD protocol is mainly used to maintain the next hop node information reaching the controller, and the TD protocol will update the information of the latest neighbor list. The TD message includes the identity information of the controller, the energy state of the node, and the number of hops required to reach the sink node. In order to broadcast the TD message to the entire network, the controller will periodically forward the TD message to the surrounding neighbor nodes. In this paper, the trust value collected by the node is uploaded to the controller in the form of a topology message to realize the report of the trust value, which can save the energy consumption of the node.

Identity Authentication of IoT Remote Control

With the increasing use of information interaction and data communication, various security issues are also increasing. During the interaction of data resources, the privacy information of IoT terminal devices, the resources, and the effective management and access of data resources are greatly threatened. In the Internet of Things environment, in order to ensure the legitimacy and privacy protection of terminal devices resources, a reasonable identity authentication method is designed, which can not only ensure the legitimacy of terminal members but also avoid the privacy information of terminal members.

Assuming that there are k positive integers that are mutually prime, let:

$$P = p_1 p_2 \cdots p_k = p_1 P_1 = p_2 P_2 = \cdots p_k P_k \tag{8}$$

Then the following congruence equations are satisfied:

$$\begin{cases} x \equiv y_1 \bmod p_1 \\ x \equiv y_2 \bmod p_2 \\ \quad \cdots \\ x \equiv y_k \bmod p_k \end{cases} \tag{9}$$

To obtain a unique solution, we have:

$$x = y_1 P_1 P_1^{'} + y_2 P_2 P_2^{'} + \cdots y_k P_k P_k^{'} (\mathrm{mod}\, P) = (\sum_{i=1}^{k} y_i P_i P_i^{'} \text{\textdiamond} \mathrm{mod}\, P \tag{10}$$

(1) Network initialization. In this work, it is assumed that the proposed model has n terminal devices.
(2) Authenticate and register terminal members before granting access to system resources by end devices.
(3) Key calculation for remote access. If the initiator u of the group key negotiation wants to access the terminal members of the attribute set for remote control, u selects the attribute sequence S and permission parameters from the information platform, then u selects a positive integer p0 and calculates the public key and sends it to the network.

$$\rho_{i,1} = (p_0 + sk_{u,k})\chi_{i,1} \tag{11}$$

$$\rho_{i,2} = p_0 \chi_{i,1} \tag{12}$$

After receiving the information broadcast by u, the terminal members with the attribute calculate the formula (13), and verify the user's identity information by formula (14):

$$\begin{cases} \delta_{i,1} = \lambda_i^{-1} \rho_{i,1} \\ l_{i,1} = \lambda_i^{-1} \rho_{i,2} \end{cases} \tag{13}$$

$$e(\delta_{i,1}, g_1) = e(l_{i,1}, g_1) e(T_{i,1}, pk_{u_j}) \tag{14}$$

The Chinese remainder theorem is a crucial result in number theory with diverse applications in fields like cryptography, coding theory, and digital signal processing. It solves the problem of finding a number that satisfies a set of modular equations with different moduli, provided that the moduli are pairwise coprime. This property makes it a valuable tool in public-key cryptography, error-correcting codes, and signal processing for efficient computation. If the equation holds, it means that x is a valid terminal member. The following equation is calculated according to the Chinese remainder theorem:

$$\begin{cases} x_i \equiv l_{i,1} (\mathrm{mod}\, p_1) \\ x_i \equiv T_{i,2} (\mathrm{mod}\, p_2) \\ \qquad \cdots \\ x_i \equiv T_{i,t} (\mathrm{mod}\, p_t) \end{cases} \tag{15}$$

and a unique solution is obtained:

$$x_i = (\sum_{v=1}^{t} l_{i,v} \bullet y_v \bullet \frac{P}{P_v}) \bmod P \tag{16}$$

The key obtained is:

$$group_{key} = x_i = (\sum_{v=1}^{t} l_{i,v} \bullet y_v \bullet \frac{P}{P_v}) \bmod P \tag{17}$$

There is exchange between terminals during remote access.

RESULTS, ANALYSIS, AND DISCUSSION

In terms of routing algorithm verification, this paper uses the i7-6700HCPU and 16GBRAM. The node promiscuous mode is opened and the sending and receiving information of the nodes is collected to calculate the basis of performance indicators such as the number of malicious node attacks and topology packet reports, and then the improved protocol is evaluated. First, 50 ordinary nodes are randomly generated (0~20%). The system operation command set mainly includes module operation commands, basic commands, and high-level commands. Module operation commands include module initialization, reading module hardware version information, reading device software versioning, and reading device hardware physical address name. The basic commands mainly provide MCU control operations on the RFID module and Mifare card at the most basic level. High level commands such as turning on the antenna, turning off the antenna, searching for cards, anti-collision mechanisms, selecting cards, password verification, card activation, card authentication, reading data blocks, writing data blocks, and card hanging are the integration of basic commands, with the aim of improving development speed and facilitating users' secondary development. For example, to read the card UID, three basic commands need to be integrated: Find Card ->Anti Conflict ->Select Card. This type of command includes read card UID, read card data block, write card data block, modify card password, and increase/decrease electronic wallet value. Some high-level command sets are shown in Table 1, Table 2, Table 3.

Table 1. Reading hardware version information

Command	START	Extend	Lc	Ins	Load	MathCheck	END
Read hardware version information	aa	00	01	02	None	03	bb
Return	16-byte hardware version number						

Table 2. Read Mifare card UID

Command	START	Extend	Lc	Ins	Load	MathCheck	END
Read UID	aa	00	01	06	None	07	bb
Return	4-byte UID						

Table 3. Reading Kn block data

Command	START	Extend	Lc	Ins	Load	MathCheck	END
Read Kn block data	aa	00	08	07	ff -- ff 6-byte password	0f	bb
Return	16-byte data of Kn block						

For IoT remote control authentication, we take the OAuth 2.0 authentication and authorization standard as the basis and provide authentication and authorization by implementing OAuth 2.0 services. In testing, we implemented a Rest API authentication and authorization project using SpringBoot framework for prototyping. At the same time, in order to control the differences in other environments as much as possible to make the experimental data more comparable, we still use the OAuth module and MySQL database attached to the spring framework to implement the OAuth2.0 authorization service. The spring framework's implementation of OAuth2.0 aims to improve security and make it possible for apps to securely connect to limited resources without having to store user credentials. As a result, the information provided with third-party applications will be better controlled. With features like support for multiple grant types, token management, and connection with spring security, the OAuth2.0 implementation in the spring framework makes it simple for developers to add permission to their applications.

Analysis of Verification Results of Secure Routing Mechanism

On the SDN-WISE software-defined IoT security framework, this paper proposes a software-defined IoT security architecture based on a trust management mechanism and realizes the detection and response of security attacks under the global network view, improving the IoT defense against malicious node attacks. This paper implements a lightweight local trust evaluation mechanism, and then utilizes the advantages of global topology, centralized control, and local trust information to achieve an efficient mechanism for isolating malicious nodes, which enables it to quickly identify malicious nodes and isolate malicious nodes at the least cost node. A lightweight local trust evaluation mechanism can be implemented in a secure routing mechanism to enhance network security by evaluating the trustworthiness of neighboring nodes based on their behavior and past interactions. This helps to identify and isolate malicious nodes, making the routing process more secure and reliable. Additionally, it ensures that sensitive information is only shared with trusted nodes, improving network efficiency and protecting it from malicious actors. It guides the data packet transmission between nodes by issuing flow tables.

As shown in Figure 5, the detection rate of malicious nodes will decrease with the increase of the proportion of malicious nodes, which is inevitable, because within the specified network range, the increase of malicious nodes will be accompanied by the decrease of ordinary nodes, which will significantly affect the trust value of the node. However, the detection rate of malicious nodes by the scheme used in this paper is better than that of the TRPL scheme, because the scheme in this paper uses the software-defined idea to detect malicious nodes through the controller and eliminates malicious nodes in the network through the controller and flow table. This greatly improves the security of the network.

In the experimental environment, as the proportion of malicious nodes increases, the probability of packets being dropped by malicious nodes also increases. When the malicious node is zero, the packet loss rate of the three schemes in the figure is less than 3%. The reason for the packet loss rate at this time is that the wireless sensor network itself is unstable. As can be seen from Figure 6, in the experimental environment, as the proportion of malicious nodes increases, the packet delivery rate of the MRHOF-RPL(Minimum Rank with Hysteresis Objective Function for RPL) protocol is most affected by malicious nodes. The packet delivery rate of the MRHOF-RPL protocol in low-power and lossy networks is severely affected by malicious nodes, which violate protocol rules and disrupt network communication. The multi-objective nature of the protocol can overlook the effects of malicious nodes on the network, resulting in a significant impact on the packet delivery rate, a crucial metric for data transmission. When the number of malicious nodes in a low-power and lossy network increases to 20%, the MRHOF-RPL protocol experiences a packet loss rate of around 55%. In contrast, the scheme proposed in this study shows no significant increase in packet loss rate. This is due to the scheme's centralized management of software-defined IoT controllers, which effectively identifies and removes malicious nodes from the network, thereby improving network communication.

Figure 5. Malicious node detection rates for different schemes

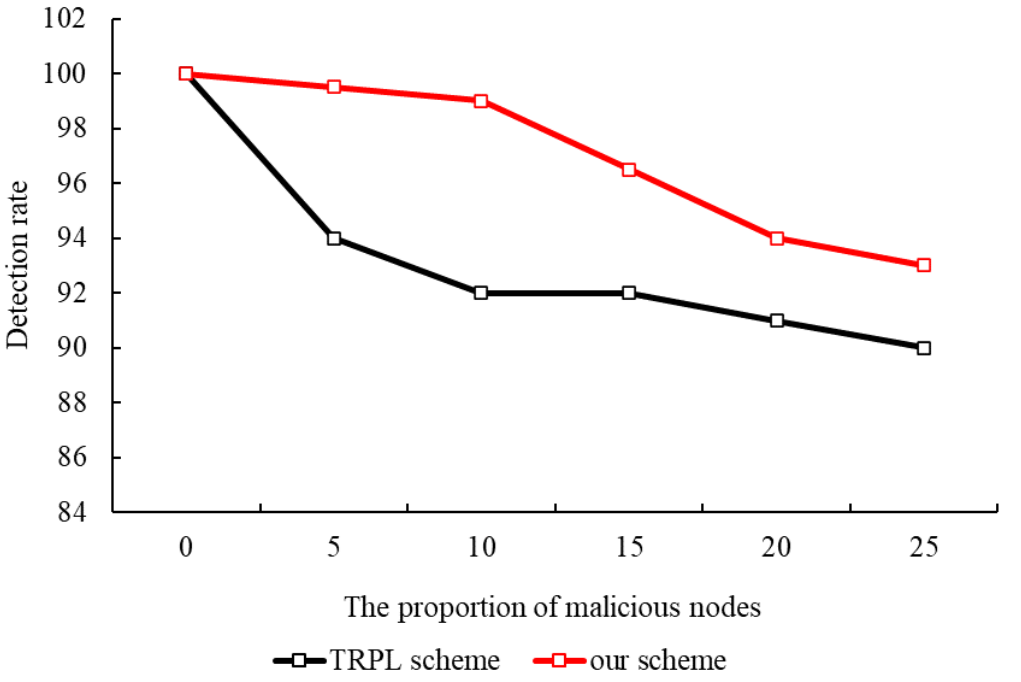


Figure 6. Packet loss rate of different schemes

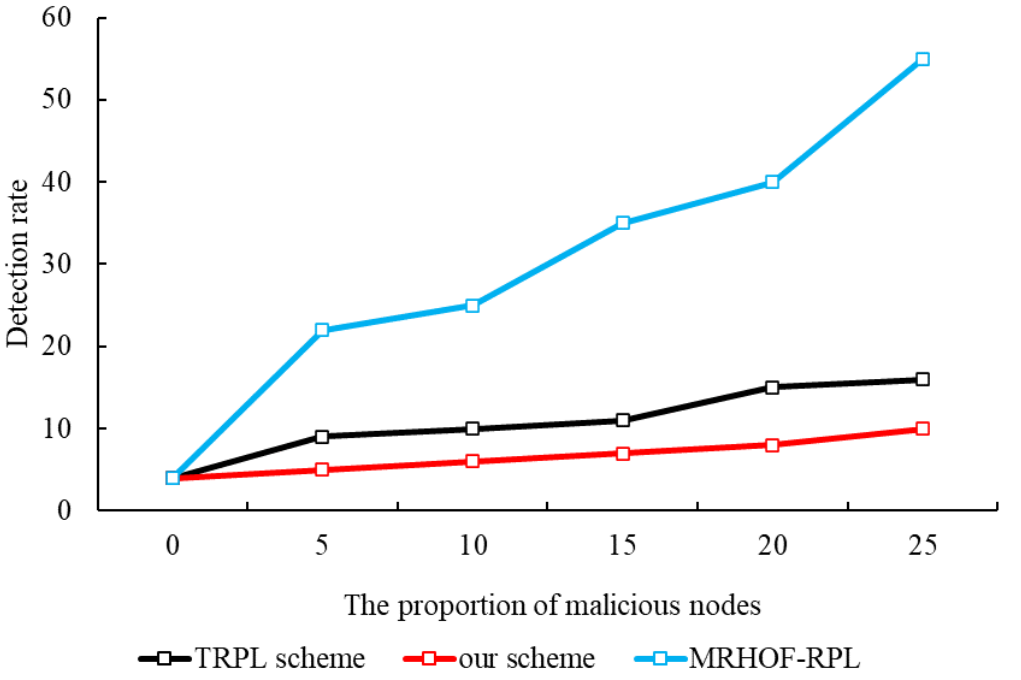
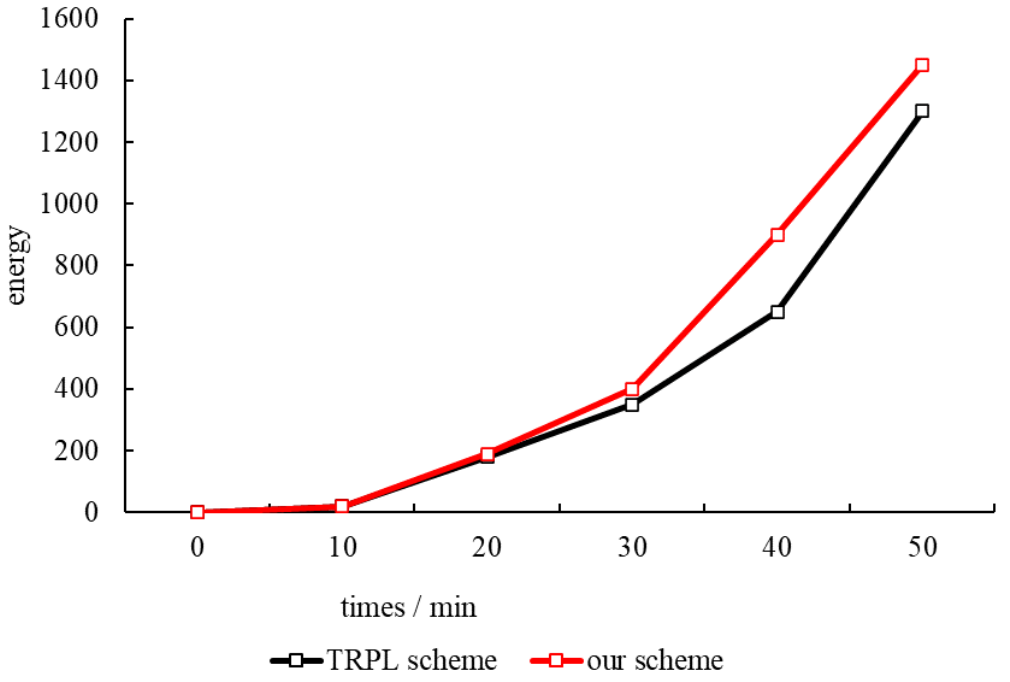


Figure 7. Energy consumption of different schemes



TRPL can also identify malicious nodes through the trust mechanism, but the effect is not as obvious as this solution with software-defined ideas, so there will be a small decline.

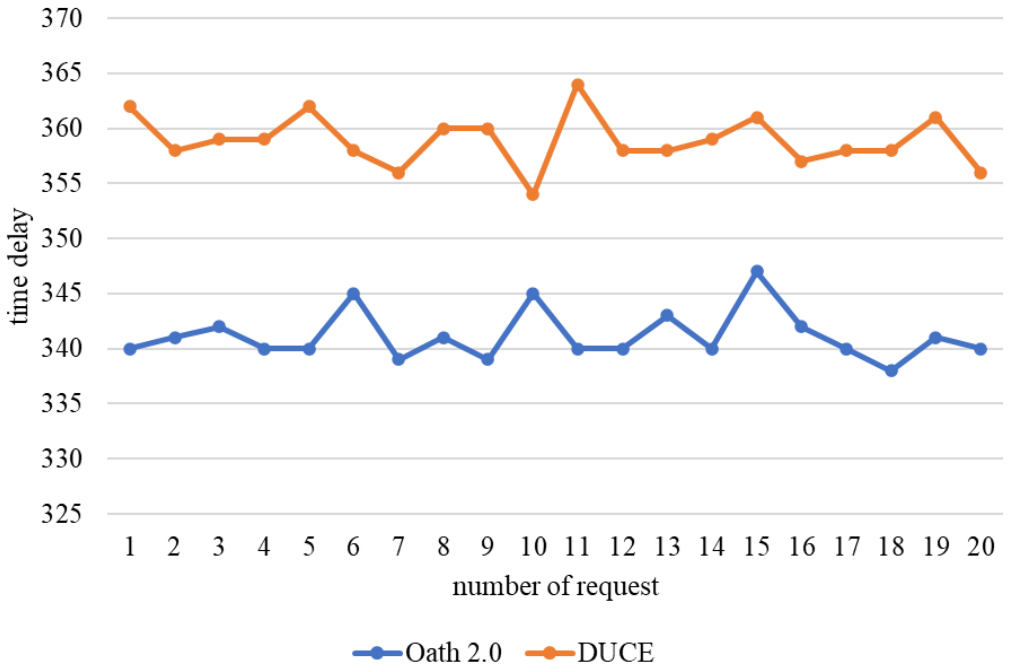
In wireless sensor networks, the batteries of sensor nodes cannot be replenished effectively, so the energy consumption parameters of nodes are very important. An energy-efficient wireless sensor protocol would bring significant benefits to the lifetime of the network. As depicted in Figure 7, the TRPL scheme requires the node to transmit information to the computing node, leading to energy consumption and thereby shortening the node's lifespan.The solution in this paper adopts the system of software-defined IoT. The collected node data only needs to be uploaded to the software-defined IoT controller, which is responsible for computing and isolating malicious nodes. Therefore, the burden on nodes can be reduced and part of the overhead can be reduced, thereby prolonging the life cycle of the network.

Analysis of Experimental Results of IoT Remote Control Authentication

Latency refers to the communication time required by the system to transmit a message from one end of the network to the other, including delays in sending, propagating, processing, and queuing. Since the processing delay and queuing delay mainly depend on the size of the communication message, we pay more attention to the transmission and propagation delay in this scheme; that is, the delay in this paper refers to the end-to-end transmission delay. Figure 8 shows the time delay comparison results of different identity authentication schemes used in remote control.

To demonstrate the effectiveness of the execution model, we first use Postman to test the propagation delay. The graph shows the results of 20 runs. We can see that all latencies in DUCE are slightly higher than OAuth 2.0. Among them, the minimum delay is increased by about 15.02%, the maximum delay is increased by about 17.54%, and the average delay is increased by about 16.3%; delays of no more than 20% makes them all within the acceptable range.

Figure 8. Comparison of transmission delay between DUCE and OAuth 2.0



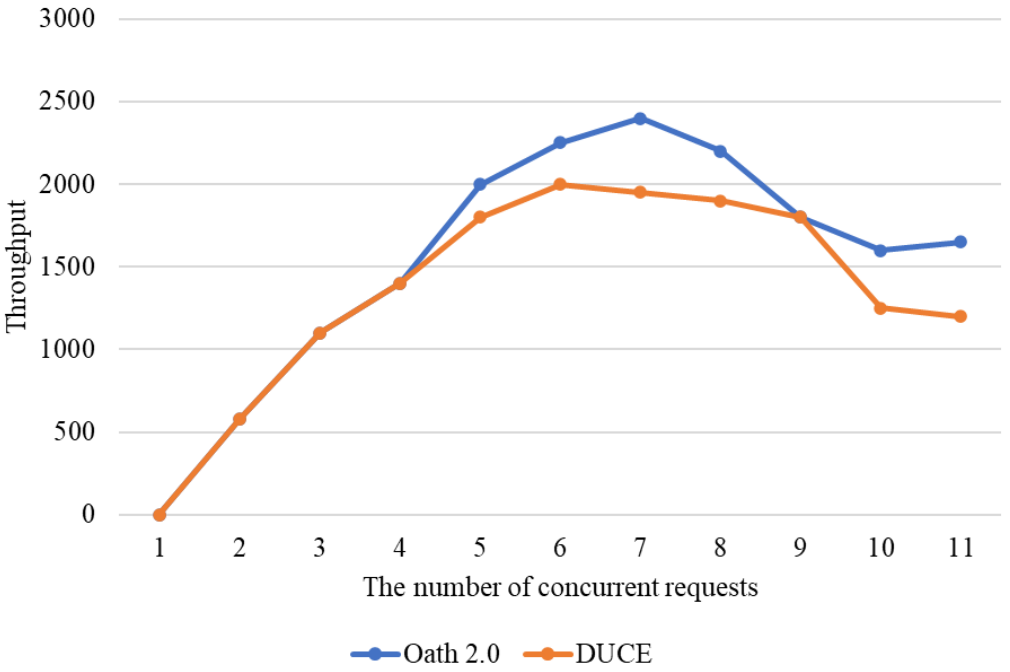
Then, we use JMeter to test the throughput of the authentication, as shown in Figure 9. Figure 9 shows the difference in authentication throughput between the baseline system and DUCE. The graph shows the average result of 20 runs. We found that the peak throughput of our solution was only about 15% lower than that of OAuth 2.0.

Based on the above experimental results, we found that implementing a new method for authentication and authorization increases latency and reduces throughput. The choice of the benchmark system OAuth 2.0 may be limited to an experimental configuration with a peak throughput performance of around 2400tps/s. In DUCE, different choices will lead to different throughput performance, and the peak throughput performance of FISCO BCOS reaches about 2000tps/s. Financial Blockchain Shenzhen Consortium (FISCO BCOS) is a blockchain platform for building consortium blockchains, while DUCE is a decentralized identity system that may use FISCO BCOS as its underlying blockchain platform. FISCO BCOS provides a secure and scalable infrastructure for blockchain applications, including decentralized identity systems. Therefore, a reduction of about 17% (less than 20%) is within the acceptable range. In other words, we demonstrate that DUCE does not introduce unbearable overhead compared to the existing OAuth, a widely used authorization solution, while preventing user privacy leakage.

CONCLUSION

This study focuses on a new type of network technology that emphasizes the importance of computer network security management. To ensure a stable and secure operation of computer networks, it is essential to meet user needs, thoroughly understand the structure of remote control systems, implement practical security management measures, and integrate remote control technology to enable scientific

Figure 9. Throughput comparison of authentication between DUCE and OAuth 2.0



equipment management. By reducing the likelihood of security issues, long-term development of IoT computer network technology in our country can be achieved.

To address this, a software-defined IoT security architecture that incorporates a trust management mechanism is proposed. This architecture enables the detection and response of security attacks from a global network perspective, thereby enhancing the IoT's ability to defend against malicious node attacks. Simulation experiments are conducted to verify the effectiveness of the proposed scheme. The experimental data analysis focuses on three aspects: the detection rate of malicious nodes, data packet loss rate, and energy consumption of the scheme. The results demonstrate that this scheme effectively identifies and isolates malicious nodes while optimizing energy consumption to ensure the normal operation of nodes and maintain good link quality.

However, there are some limitations of this paper. First, the specificity of the experimental environment and equipment may make the results not applicable to all situations, as different network configurations, hardware devices, and communication environments may have an impact on the results. Second, the limited nature of the data sample may lead to biased results or be insufficient to support generalized conclusions, thus a broader and more diverse data sample may provide more comprehensive conclusions. Future research directions should consider expanding the scope and diversity of experimental environments and consider more diverse network configurations.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

FUNDING STATEMENT

This work was supported by the Guangxi College and University Young and Middle-Aged Teachers Scientific Research Basic Ability Improvement Project 2021 Annual Project: Research on the Design and Key Technologies of Anti-Drawing Attachment Devices for 3D Printers, Project No. 2021KY1067.

REFERENCES

Aggarwal, N., Albert, L. J., Hill, T. R., & Rodan, S. A. (2020). Risk knowledge and concern as influences of purchase intention for internet of things devices. *Technology in Society*, *62*, 101311. doi:10.1016/j.techsoc.2020.101311

Al-Sibai, H. S., Alrubaie, T., & Elmedany, W. M. (2021). IoT cybersecurity threats mitigation via integrated technical and non-technical solutions. *International Journal of Electronic Security and Digital Forensics*, *13*(3), 298–333. doi:10.1504/IJESDF.2021.114957

Aldaej, A. (2019). Enhancing cyber security in modern internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI). *IEEE Access : Practical Innovations, Open Solutions*.

Alkali, Y., Routray, I., & Whig, P. (2022). Strategy for reliable, efficient and secure IoT using artificial intelligence. *IUP Journal of Computer Sciences*, *16*(2), 16–25.

AlkaliY.RoutrayI.WhigP. (2022). Study of various methods for reliable, efficient and secured IoT using artificial intelligence. SSRN 4020364. 10.2139/ssrn.4020364

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly*, *36*(2), 346–357. doi:10.1016/j.giq.2018.09.007

Chen, L. (2021). Application of computer network communication technology in production and life. [IOP Publishing.]. *Journal of Physics: Conference Series*, *1744*(3), 032161. doi:10.1088/1742-6596/1744/3/032161

Chu, M., & Song, Y. (2021). Analysis of network security and privacy security based on AI in IOT environment. *The 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*. IEEE.

Dovhan, A. D., Bernaziuk, Y. O., & Tkachuk, T. Y. (2019). Internet of things technologies in medical sector: Cyber security issues. *Wiadomosci Lekarskie, 72*(12, 2), 2563-2567.

He, X. (2021). RETRACTED: Analysis of network intrusion detection technology based on computer information security technology. [IOP Publishing.]. *Journal of Physics: Conference Series*, *1744*(4), 042038. doi:10.1088/1742-6596/1744/4/042038

Heriadi, H., & Pamuji, G. C. (2020). Cyber security in IoT communication (Internet of Things) on smart home. [). IOP Publishing.]. *IOP Conference Series. Materials Science and Engineering*, *879*(1), 012043. doi:10.1088/1757-899X/879/1/012043

Isravel, D. P., Arulkumar, D., & Angelin, A. C. (2018). Cyber security threats and risk mitigation measures in internet of things. *International Journal of Civil Engineering and Technology*, *9*(10), 1619–1628.

Javed, S. H., Ahmad, M. B., Asif, M., Almotiri, S. H., Masood, K., & Ghamdi, M. A. A. (2022). An intelligent system to detect advanced persistent threats in industrial Internet of Things (I-IoT). *Electronics (Basel)*, *11*(5), 742. doi:10.3390/electronics11050742

Kashiyama, M., Kashiyama, R., Seki, H., & Hosono, H. (2021). Study on cyber-security for IoT edge utilizing pattern match accelerator. *Electrical Engineering in Japan*, *214*(2), e23333. doi:10.1002/eej.23333

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. doi:10.1016/j.ijcip.2019.01.001

Li, Y. (2013). Design of a key establishment protocol for smart home energy management system. *The 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*. IEEE. doi:10.1109/CICSYN.2013.42

Lixin, Z. (2017). Application analysis of data encryption technology in computer network communication security. *Computer Knowledge and Technology: Experience Skills*.

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. *Energy Reports*, *7*, 8075–8082. doi:10.1016/j.egyr.2021.07.078

Sitaraman, G. (2022). The regulation of foreign platforms. *Stanford Law Review*, *74*, 1073.

Thota, C., Mavromoustakis, C., & Mastorakis, G. (2023). CAP2M: Contingent anonymity preserving privacy method for the Internet of Things services. *Computers & Electrical Engineering*, *107*, 108640. doi:10.1016/j.compeleceng.2023.108640

Tzafestas, S. G. (2012). *Intelligent systems, control and automation: Science and engineering*.

Wu, Y., Wu, Y., Guerrero, J. M., & Vasquez, J. C. (2021). A comprehensive overview of framework for developing sustainable energy internet: From things-based energy network to services-based management system. *Renewable & Sustainable Energy Reviews*, *150*, 111409. doi:10.1016/j.rser.2021.111409

Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *Journal of the Franklin Institute*, *358*(1), 172–192. doi:10.1016/j.jfranklin.2019.02.011