applied sciences

MDPI

Article

Securing SCADA Energy Management System under DDos Attacks Using Token Verification Approach

Yu-Sheng Yang [1], Shih-Hsiung Lee [2,*], Wei-Che Chen [3], Chu-Sing Yang [3], Yuen-Min Huang [1] and Ting-Wei Hou [1]

[1] Department of Engineering Science, National Cheng Kung University, Tainan City 701, Taiwan; n98991108@mail.ncku.edu.tw (Y.-S.Y.); huang@mail.ncku.edu.tw (Y.-M.H.); houtw@mail.ncku.edu.tw (T.-W.H.)
[2] Department of Intelligent Commerce, National Kaohsiung University of Science and Technology, Kaohsiung City 824, Taiwan
[3] Institute of Computer and Communication Engineering, National Cheng Kung University, Tainan City 701, Taiwan; q36084214@gs.ncku.edu.tw (W.-C.C.); csyang@ee.ncku.edu.tw (C.-S.Y.)
* Correspondence: shlee@nkust.edu.tw; Tel.: +886-7-381-4526

Abstract: The advanced connection requirements of industrial automation and control systems have sparked a new revolution in the Industrial Internet of Things (IIoT), and the Supervisory Control and Data Acquisition (SCADA) network has evolved into an open and highly interconnected network. In addition, the equipment of industrial electronic devices has experienced complete systemic integration by connecting with the SCADA network, and due to the control and monitoring advantages of SCADA, the interconnectivity and working efficiency among systems have been tremendously improved. However, it is inevitable that the SCADA system cannot be separated from the public network, which indicates that there are concerns over cyber-attacks and cyber-threats, as well as information security breaches, in the SCADA network system. According to this context, this paper proposes a module based on the token authentication service to deter attackers from performing distributed denial-of-service (DDoS) attacks. Moreover, a simulated experiment has been conducted in an energy management system in the actual field, and the experimental results have suggested that the security defense architecture proposed by this paper can effectively improve security and is compatible with real field systems.

Keywords: SCADA security; DoS attack; token verification; energy management system

check for updates

Citation: Yang, Y.-S.; Lee, S.-H.; Chen, W.C.; Yang, C.-S.; Huang, Y.-M.; Hou, T.-W. Securing SCADA Energy Management System under DDos Attacks Using Token Verification Approach. *Appl. Sci.* **2022**, *12*, 530. https://doi.org/10.3390/app12010530

Academic Editor: Pericle Perazzo

Received: 5 December 2021
Accepted: 4 January 2022
Published: 5 January 2022

1. Introduction

The Industrial Internet of Things (IIoT) or Industry 4.0 has led to constant exploration and development in new industrial control and monitoring, industrial automation, working service process, data analysis of assembly lines, and new commercial models. There are many successful and actual examples available in relevant studies, such as adopting the Supervisory Control and Data Acquisition (SCADA) [1] system and the Programmable Logic Controller (PLC) [2] to establish a reservoir control system [3]. Hence, the Industrial Control System (ICS) [4] is perceived as playing a critical role in technological transitions and national security. Due to the special features of IIoT, damages caused by information security threats can easily go beyond the internet and cause substantial destruction. In the communication platform of the Industrial Internet of Things, Local Operating Networks (LON) is a common automation and monitoring network architecture classical solution. In addition, in the media access control (MAC) layer, how to avoid conflicts and cause unfair sharing of network bandwidth between devices (communication nodes) is an important issue. P-persistent CSMA (Carrier Sense Multiple Access) scheme is usually easy to cause possible bandwidth allocation unfair problem between competing nodes. The authors of [5] analyzed that in most network traffic scenarios, unfairness is the shortcoming of predictive p-persistent CSMA operations. It also proves that the average bandwidth available to a node is a linear function of its degradation state and does not depend on the degradation state of other sites. Aiming at the unfairness of random access in the Industrial Internet of Things, the authors of [6] further studied the deviation of the site from the defined competition mechanism in CSMA/CA (Collision Avoidance), and used Bianchi model to estimate that this deviation affected network throughput. It shows that the fairness of the network is seriously affected. Moreover, the dynamic average discounted payoff mechanism of game theory is used to solve the problem of network throughput allocation. It can be seen that the quality of service (QoS) of the network plays an important role in the industrial Internet of Things. When the nodes generate a large amount of data, the media access control (MAC) layer protocol does not perform well in terms of fairness and throughput. Because the MAC layer does not have the capacity to provide QoS for priority or forwarding flows. Therefore, it is not easy to be detected when the device is attacked. The authors of [7] proposed a QoS-IoT architecture and developed an adaptive contention window (CW) algorithm for evaluation of the effectiveness of fairness, throughput and utilization in medium access control. In addition, the attack detection, fairness, throughput and buffer utilization are evaluated through the simulation of Sybil attack. The experiments in [7] show that QoS-IoT has significant performance.In addition, in QoS, attacks on the application layer of the network architecture are also quite common.Among the threats to information security, DoS is an attack specifically designed to paralyze a certain network, device, or source. During one kind of DoS attack, DDoS uses a number of intrusive devices, namely, botnets, to attack a target system and paralyze its network or processor through an intensive operation; for example, the botnet Mirai [8] has paralyzed many famous networks and online services. Though this virus did not impact the industrial sector, it revealed how DDoS attacks could cause possible devastating consequences. Moreover, as the source code of this virus has been published online and the DDoS service is emerging, many other attacks targeting IoT and other basic IoT architectures are expected to be seen in the future. By using the same token, an intruded ICS system would eventually become a member of the botnets, which could be used as a tool for hackers to attack other enterprises.

The Energy Management System (EMS) [9] is a service for monitoring, managing, and controlling energy. The growing maturity of IIoT technology has resulted in many new applications; for example, the Building Energy Management System (BEMS) [10] has been applied in resident-centered housing together with the demand response (DR) to balance the supply and demand of power and avoid energy waste [11]. The smart green energy management system covers a wide range of technologies, including SCADA, CEMS, BEMS, PLC, and IIoT technology. At present, the difference between Operational Technology (OT) and Information Technology (IT) [12] represents the major reason why enterprises in the IIoT sector pay little attention to information security. Basically, IIoT uses physical isolation and is separated from the external network, which means enterprises may be attacked by external viruses due to administrative negligence and uncertainty in physical isolation. Previously, OT and IT had separate environments, and each had its own responsibilities. Today, as the growing availability of the internet enables the two systems to gradually connect with each other, the nature and architecture of OT and IT are different and the existing management and implementation method for information security may not be effective in defending against attacks; for example, as ICS must be in constant operation, it is relatively difficult to stop it for a security update and may cost a lot of money. Moreover, it takes ten minutes or more for some ICS systems to restart after powering off and major losses may be incurred during this period. In terms of product life expectancy, while ICS can be used for a long time, ranging from 10 years to 20 years, the design and manufacture of these systems do not consider information security; therefore, updating and replacing hardware and software, as well as installing, updating, and fixing programs in ICS, is very difficult. In addition, the network device that ICS connects with may have insufficient defense capability and fail to detect and process malicious traffic or large common traffic.

In the environment of the Internet of Things, due to the interconnection of a large number of devices, it is a common method to prevent unknown malicious attacks through authentication protocols. In the issue of authentication, there are many solutions and considerations. First of all, in the application of sensors, the solution must take into account that the trade-offs between lightweight, low power consumption and security. In addition, how the authentication mechanism prevents potential attacks such as Sybil, replay, password guessing, message forgery, man-in-the-middle, and DoS is also an important feature of the evaluation. In [13], it is mentioned that the authentication scheme needs special consideration of distributed denial of service attacks. In particular application scenarios, location and privacy need to be considered. In practical deployment, the authentication solution must be scalable, and involving the three-layer architecture (perception layer, network layer and application layer) of the Internet of Things, and the ability to add new devices without any further settings or configuration. The authentication methods of the Internet of Things are mainly divided into hardware-based (True Random Number Generator (TRNG), Physical Unclonable Function (PUF) and Trusted Platform Module (TPM)), token-based and procedure (one-way, two -way and three-way) [13]. The authors of [14] proposed an xTSeH (TPM extension scheme) architecture using TPM modules to implement a shadow TPM in the form of kernel modules to ensure integrity. Due to the limitation of hardware capabilities, not all IoT devices can be equipped with TPM chips. Therefore, Trusted Booting Protocol (TBP), Remote Verification Protocol (RVP) and Node Authentication Protocol (NAP) are mainly used to achieve integrity verification and authentication between devices. Accordingly, using PUF of hardware-based solution is a current trend because it has advantages over software-based solution. The authors of [15] proposed a lightweight PUF authentication technology, using simple bitwise operations along with a PUF circuit and a true random number generator (TRNG), avoiding the use of any encryption or hash functions, and passing challenge-response authentication protocol. However, PUF's lightweight security solutions usually lack security functions (such as vulnerabilities for Dos attacks) and are relatively costly. Therefore, the combination of software solutions (low cost) and hardware solutions (more secure) should be considered and applied in different situations at the same time. The solution we proposed is deployed in the actual field by using the trusted encryption verifier module (TEVM) to integrate between the SCADA server and the TCP-RTU converter. TEVM architecture can achieve scalability and does not affect the operation of existing systems. Adding to this, TEVM has both cost and efficiency merits.

The system architecture proposed in this paper has been applied in the national infrastructure with strict requirements for security. Defenses against DoS attacks usually include attack inspection, traffic filtration, and multiple verifications. In order to address the aforesaid problems, this paper proposed an encrypted verification mechanism based on tokens and the transport layer security (TLS) protocol [16] to prevent hackers using the external internet to attack firewalls and Intrusion detection and prevention systems (IDPS), access the BEMS, and successfully use DoS attacks against the SCADA Server. The contribution of this paper has been applied and verified in the energy management system of a Smart Green Energy Science City in southern Taiwan; thus, it is proved that DoS attacks can be effectively defended by adding an encrypted verification mechanism. In addition, spending a bit more in the calculation, transmission, and storage can prevent the system's control system from failing to capture a device's response and sending repetitive requests, which may cause errors due to the inability to access device information and even overwhelm the system. According to experimental results, the security defense architecture proposed in this paper is effective in improving security and compatible with real field systems.

Other parts of this paper are arranged as follows: the second part reviews relevant studies, the third part defines the problems to be solved, the fourth part introduces the trusted encrypted validator module (TEVM), which is based on the token authentication architecture proposed by this paper, and the fifth part reveals the experimental results and concludes the paper.

2. Related Work

2.1. The Authentication of the Industrial Internet of Things

The SCADA system is usually realized by integrating the Modbus industrial communication protocol. However, Modbus is designed to be fast and convenient, and only considers its use in the local network and the use of plaintext to transmit packets. With the increasing demand for automated industrial control systems, SCADA has moved from a strictly isolated network to a highly interconnected Internet. Therefore, the advantages of Modbus protocol in the past will cause serious security breach in modern application scenarios. Furthermore, the infrastructure is exposed to information security risks, which may be attacked by hackers at any time, causing significant economic losses. The authors of [17] proposed a mechanism for the authentication of industrial control systems. During the transmission of Modbus TCP/IP packets, the hash code of authentication is generated by intercepting the header fields of the TCP packet to confirm the identity of the device. Obviously, in the SCADA system, it is not sufficient to use only Modbus TCP/IP packet content for authentication. The authors of [18] proposed an automated validation of Internet security protocols and applications (AVISPA) tool that is used in the authentication and key agreement protocol of the Industrial Internet of Things (Industry 4.0). AVISPA is based on a layered approach protocol design, and uses ECC (Elliptic Curve Cryptography), PUF, hash function, concatenation, and XOR operations to provide mutual authentication between IoT nodes and centralized nodes. AVISPA can effectively resist DoS, replay and spoofing attacks. In the resource-constrained smart meters application scenario, the authors of [19] use fully hashed menezes-qu-vanstone key exchange mechanism along with Elliptic curve cryptography and one-way hash functions to provide trust, anonymity and mutual authentication, and reduce energy, communication and computing costs. In [20], this research work further proposed a lightweight remote device mutual authentication and key exchange model, which is applied in IIoT, named MAKE-IT. MAKE-IT uses symmetric and asymmetric key encryption, hash and timestamp technologies to perform mutual authentication and effectively defend against replay attacks, modification attacks and man in the middle attacks. It shows that in the security issues of the Industrial Internet of Things, how to use a lightweight authentication mechanism to effectively resist attacks is an important key factor.

2.2. The Denial of Service Attacks on Industrial Internet of Things

The Industrial Control System (ICS) is the core of IIoT and how to improve its reliability and security has become an important topic. A denial of service attack is common in the IIoT environment and attackers usually send a lot of ineffective data to receivers to destroy the SCADA system’s ability to function properly, meaning its devices fail to operate according to normal programs, and the absence of proper defense can result in serious losses. In terms of the threats and breaches faced by the ICS system, [21] proposed that, with the development of IoT and communication technology, the IIoT control system is no longer closed. Stute et al. [22] put forward LIDOR, which is a safe and lightweight multihop communication protocol that uses effective symmetric keys to encrypt and protect the transfer of data packets. The protocol proposed in this study can also defend against the known packet dropping DoS attack model. Borgiani et al. [23] designed distributed congestion control by duty-cycle restriction (D-ConCReCT) to conduct congestion control examinations and lower the DoS attack risk in IIoT. Ref. [24] introduced fog computing as the medium for the smart micrograds system and used the average consensus-based algorithm for scheduling tasks to reduce the impact of DoS attacks. To this end, this paper proposed a Trusted Encrypted Validator module (TEVM) based on token authentication to lower the probability of the SCADA system being attacked by DoS.

2.3. The Authentication for DoS Defense in IoT Environment

Ghosh et al. [25] pointed out that the major threats in the SCADA system are its application of a lightweight private key exchange mechanism and the absence of an attack defense service; therefore, establishing a prevention mechanism for SCADA should adopt encrypted keys, which is important for authentication and authorization of access. Lyu et al. [26] proposed employing selective authentication-based geographic opportunistic routing (SelGOR) against DoS attacks, which ensures the integrity of data on the basis of entropy information, isolates DoS attacks, and reduces the calculation cost through distributive coordinated authentication. In addition to employing the identity authentication protocol, Ghahramani et al. [27] also adopted users' misbehavior and the received signal strength indicator to achieve solutions for energy saving, prevent DoS attacks, and locate the attacker in the applied IoT scenario. Regarding the token-based proposal, tokens are remarkably resilient to achieve the authentication and authorization mechanism. In addition, tokens are issued by a third-party authentication center, which could improve its reliability and security. Moreover, tokens feature great privacy protection, and ensure that sensitive information would not be disclosed easily. Ref. [28] created Token-based Lightweight User Verification (TBLUA) to enhance the strength and security of identity authentication. Therefore, the keys to achieving IIoT security include low calculation costs, low communication and storage costs, achieving identity authentication, and preventing attacks. In this context, this paper proposed an encrypted authentication mechanism with a Trusted Encrypted Validator Module (TEVM), based on token authentication and the transport layer security (TLS) protocol, to improve SCADA's defense against DoS attacks.

2.4. The DDoS Attack Tools

A distributed denial of service attack is an attack that maliciously reduces the performance of a website or server. Distributed attack uses multiple computers in a distributed network to use DoS to attack the target website or server. Multiple computers send a large number of fake requests to the target. Targets are flooded with such requests, making legitimate requests or users unable to use resources. The types of DDoS attacks can be roughly divided into volume-based attacks, protocol attacks, and application layer attacks. Attack methods include UDP flood, ICMP flood, SYN flood, Ping of Death, Slowloris, NTP Amplification and HTTP flood. The HTTP Unbearable Load King (HULK) DDoS attack tool [29] will have devastating consequences when implemented, because it is executed in a form to evade most firewall rules. HULK generates unique and obscure traffic, so the authentication mechanism can effectively block HULK attacks. The Slowloris attack tool [30] is to send authorized HTTP traffic to the server. For the evaluation of parameters such as attack time, traffic rate and packet size [31], Slowloris makes the attack at a slow rate, so it is easy to detect the traffic as abnormal and block it. The LOIC attack tool [32] is mainly to send UDP, TCP and HTTP requests to the server. The HIVEMIND mode of LOIC tool will allow remote control of other computers in the Zombie network. LOIC tool is very easy to use, and the target website can be defeated and stop responding to actual requests within a few seconds. Therefore, this paper uses LOIC tools to quickly simulate the experimental situation.

3. Problem Definition

As shown in Figure 1, the energy management system mainly consists of a power company system, a community energy management system, a building energy management system, a firewall, and IDPS and SCADA systems. The experiment of this paper was conducted in the energy management system of a Smart Green Energy Science City in southern Taiwan. When hackers use external attacks to break through a firewall and Intrusion IDPS, and there is no security defense mechanism, they can paralyze the SCADA system through DoS attacks. This can cause the system's control program to be unable to acquire the device's response and send repetitive requests, which further leads to errors due to the lack of device information and results in a hazardous impact on the energy management system. Therefore, this paper conducted a simulated experiment to prove the viability of the proposed Trusted Encrypted Validator module (TEVM), based on the token authentication architecture.

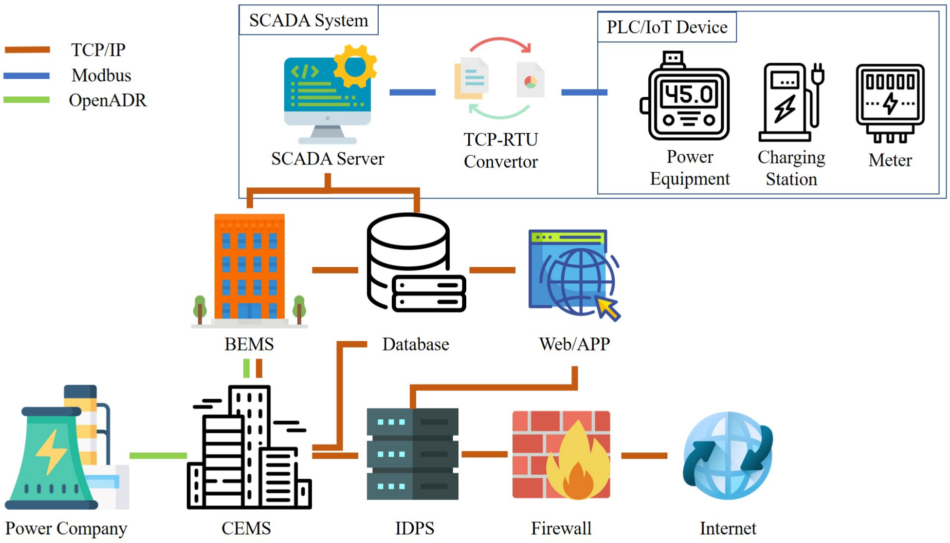


Figure 1. Energy management system in southern Taiwan.

4. Trusted Encrypted Validator Module (TEVM) Based on Token Authentication

As can be seen in Figure 2, a server named Token-based Authentication Service (TBAS), which is responsible for generating tokens for legitimate devices, was added to the SCADA system architecture. In addition, a Trusted Encrypted Validator module (TEVM) machine was added to the TBAS system to encrypt, decode, and verify the device's legality. As the major medium applied program of the SCADA server, the Control Server (CS) was in charge of controlling IoT devices, and the secure connection among CS, TEVM, and TBAS was achieved through encryption by TLS 1.3. This paper proposed a solution named the encrypted authentication mechanism, which could address security problems in two ways; the first encrypts Modbus TCP through Transport Layer Security 1.3, meaning hackers could not access or modify the content, and the second verifies CS and IoT devices through tokens to stop hackers from paralyzing the SCADA system through DoS attacks.

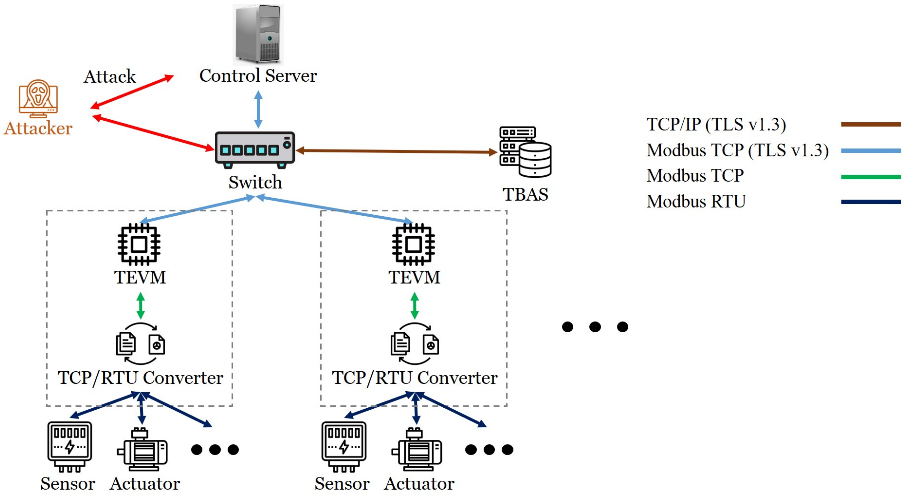


Figure 2. The proposed architecture.

4.1. Authentication Mechanism

Above all, prior to CS sending out regular requests or control requests from BEMS, the TEVM would check to determine whether the token is legitimate. If the token did not exist or was illegitimate, then, CS must apply for a legitimate token and provide the required information to TBAS during application. Upon receiving the application from CS, TBAS would examine its information legality, and if legitimate, the token would be generated and sent simultaneously to CS and TEVM, if not, CS would receive a message explaining the wrong information and the need to reapply. After receiving the message from CS, TEVM determines whether the token is legitimate and consistent with that from TBAS. If so, the requested information would be sent to the PLC/IoT Device; if not, a message explaining the incorrect information would be sent to CS accompanied by a request to reapply for the token. After receiving such requests, PLC/IoT devices are required to take immediate and specific actions, and send reply messages to TEVM. Then, after receiving this reply, TEVM would examine if there was legitimate token within itself. If there was no legitimate token, it would send the requested information to TBAS to apply for a token; if a legitimate token existed, it would send the combined token and reply to CS. After receiving the application for a token from TEVM, the TBAS procedure would follow the same procedure used when CS applied for a token. Finally, when CS received information from TEVM, it would also check whether the token was legitimate and consistent with that of TBAS. If an inconsistency is found, it would reject the message and reply to TEVM with the wrong information and a request to reapply; otherwise, TBAS would save the replied information to the database. The complete procedure of the identity authentication mechanism is shown in Figure 3.

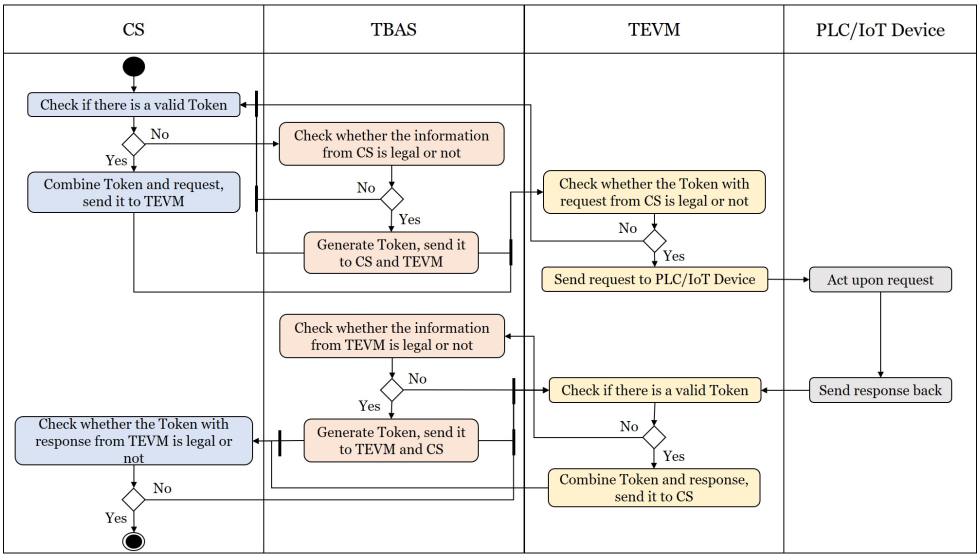

CS
TBAS
TEVM
PLC/IoT Device
Check if there is a valid Token
No
Yes
Combine Token and request, send it to TEVM
Check whether the information from CS is legal or not
No
Yes
Generate Token, send it to CS and TEVM
Check whether the Token with request from CS is legal or not
No
Yes
Send request to PLC/IoT Device
Act upon request
Send response back
Check whether the information from TEVM is legal or not
No
Yes
Generate Token, send it to TEVM and CS
Check if there is a valid Token
No
Yes
Combine Token and response, send it to CS
Check whether the Token with response from TEVM is legal or not
No
Yes

Figure 3. The authentication flow.

4.2. Generating Token

Tokenization [33] has been widely applied in various sectors, such as network communication, information security, and credit card and third-party authentication. With the help of tokenization, an internet-connected device can be projected to a token, thus becoming a reference (identification code) without external meaning or use, which can be applied in sensitive data protection, safe storage, auditing, identification, and authentication, as well as services. When other devices apply for a token through TBAS in the future, they will follow the same rule to deliver information to TBAS to obtain a legitimate token. After receiving an application, TBAS examines the seven items, generates the token if all items are legitimate, and sends a reply. If one of the seven items is incorrect, a message of incorrect information will be returned with a request for reapplication. The required items to apply for a token include the IP address (source) of the device, the applicant's hostname and mac address, the IP address (destination), socket port, hostname, and TEVM mac address as shown in Table 1. Then, based on the abovementioned seven pieces of information, TBAS generates a group of tokens through RSA-2048 and SHA-256. In addition, tokens carry an extra information packet that includes the generated time and effective period of the token, the applicant's IP and mac address, and information regarding the privilege and type of token. Both CS and TEVM are required to examine the legality of a token before combining the token and the application and sending a reply, as well as after receiving the other side's information. If all nine items (token hash value and other eight information items) are legitimate as shown in Table 2, the token is legitimate; otherwise, the token is illegitimate.

Table 1. The information for applying token

Item	Description
src_ip	the IP of the applicant (device)
src_hostname	the hostname of the applicant
src_mac_addr	the mac address of the applicant
dst_ip	the IP of the verifier
dst_port	the socket port of the verifier
dst_hostname	the hostname of the verifier
dst_mac_addr	the mac address of the verifier

Table 2. The information of token

Item	Description
iss	TBAS represented here by the IP of TBAS
iat	the time when the token was generated
exp	the expiry date of the token
aud	the IP of the applicant
hostname	the hostname of the applicant
mac_addr	the mac address of the applicant
priority	the priority of the token
service_type	the type of the token

5. Experiment

5.1. Simulation of Experimental Environment

During practical operation, this study adopted a physical server as the control server to send the access requests of IoT devices. One Raspberry Pi was adopted in TBAS to examine the legality between the control server and IoT devices and generate token in accordance with the results. Another Raspberry Pi was employed in TEVM to encrypt and decode pockets and verify the module. An ICP DAS tGW-735 device was used in the TCP/RTU Converter. The IoT devices used the temperature and humidity sensor of ICP DAS DL-100TM485. The simulated experimental environment is shown in Figure 4, and the actual environment is displayed in Figure 5.

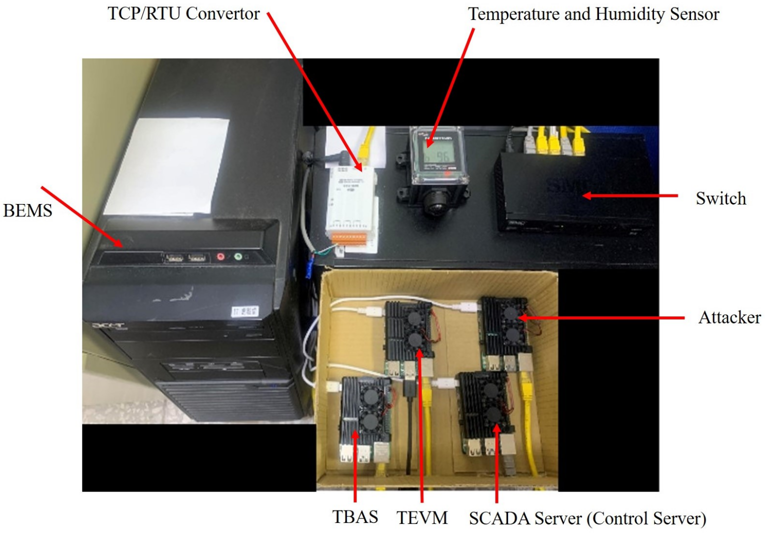

TCP/RTU Convertor
Temperature and Humidity Sensor
BEMS
Switch
Attacker
TBAS
TEVM
SCADA Server (Control Server)

Figure 4. The setup of simulation environment.

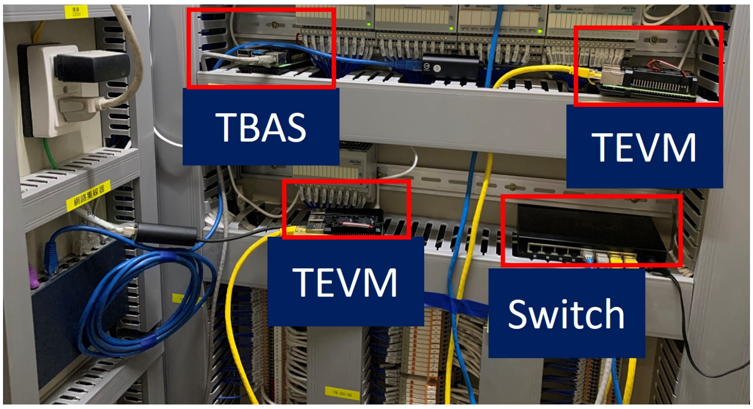
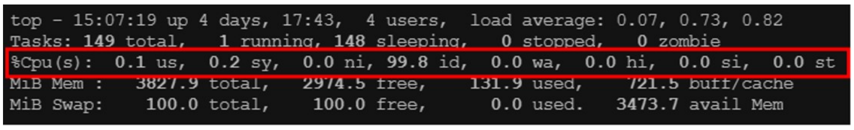


Figure 5. The setup in real energy management system.

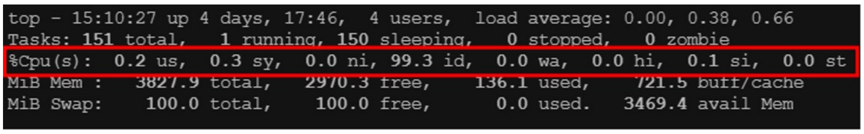
5.2. *Verifying the TEVM Mechanism*

Before verifying the effective defense of TEVM against DoS attacks, it should be proved that the SCADA system can be influenced by DoS attacks when there is no security mechanism. As the denial-of-service attack would exert an extraordinary burden on the CPU, this study explored the influence of an attack according to the usage frequency of the CPU. In addition, this paper adopted Top, which is an instant analysis tool built in the Linux system, to examine the usage frequency of the CPU. Prior to adding the TEVM mechanism to the SCADA server, when the system was idle, this study recorded some of the major information among all system parameters, as shown in Figure 6: (1) us: the percentage of the CPU used by the user space in the Linux system; (2) sy: the percentage of the CPU used by the kernel space in the Linux system; and (3) id: the idle percentage of the CPU. Before adding the TEVM mechanism, the SCADA server accessed the high frequency usage information in the single temperature and humidity sensors, which presented the usage conditions of various system parameters when taking corresponding actions per the BEMS request. As shown in Figure 7, the CPU usage percentage was 99.3% idle; thus, while the SCADA server was running, it was not busy. However, Figure 8 shows the situation of integrating the TEVM mechanism into the SCADA server; in this case, us, sy, and id account for 3.6%, 0.4%, and 96%, respectively, which indicates that running this mechanism would not have a huge impact on the SCADA server.



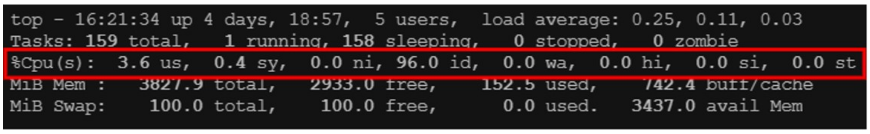
```
top - 15:07:19 up 4 days, 17:43,  4 users,  load average: 0.07, 0.73, 0.82
Tasks: 149 total,   1 running, 148 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.1 us,  0.2 sy,  0.0 ni, 99.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3827.9 total,   2974.5 free,    131.9 used,    721.5 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3473.7 avail Mem
```

Figure 6. The system information of SCADA server in idle status.



```
top - 15:10:27 up 4 days, 17:46,  4 users,  load average: 0.00, 0.38, 0.66
Tasks: 151 total,   1 running, 150 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.2 us,  0.3 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   3827.9 total,   2970.3 free,    136.1 used,    721.5 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3469.4 avail Mem
```

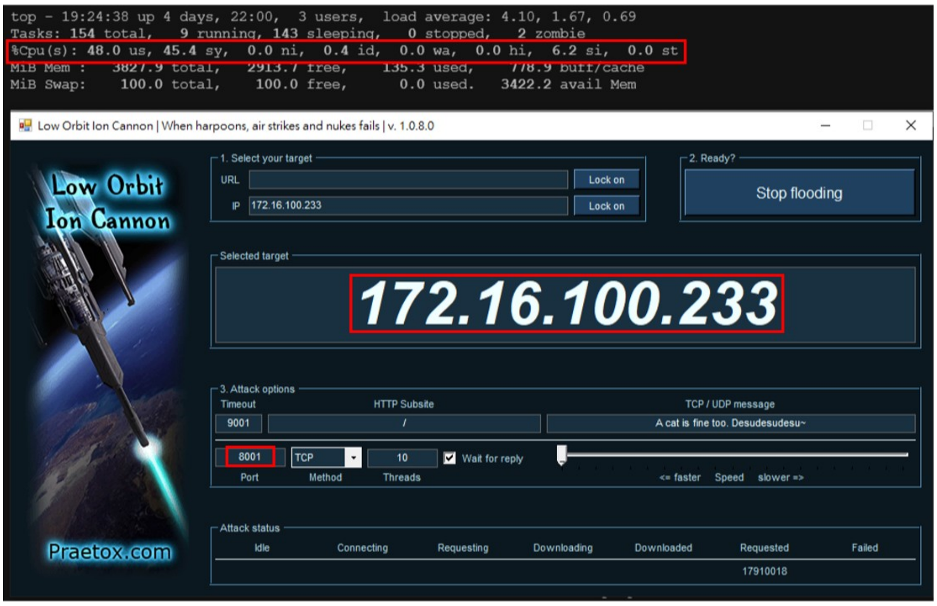
Figure 7. The system information of SCADA server in status of accessing sensor.



```
top - 16:21:34 up 4 days, 18:57,  5 users,  load average: 0.25, 0.11, 0.03
Tasks: 159 total,   1 running, 158 sleeping,   0 stopped,   0 zombie
%Cpu(s):  3.6 us,  0.4 sy,  0.0 ni, 96.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3827.9 total,   2933.0 free,    152.5 used,    742.4 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3437.0 avail Mem
```

Figure 8. The system information of SCADA server in status of accessing sensor with TEVM mechanism.

Later in the experiment, the BEMS was used as the attack node to launch the denial-of-service attacks through the LOIC tools on SCADA servers without a preventive mechanism, but with the TEVM mechanism. Figure 9 demonstrates the situation without any defensive mechanism; the us and sy values were much higher than the common values, and the id value was close to zero, which indicates that the denial-of-service attack could paralyze the CPU, and render it incapable of possessing other tasks. Hence, it can be concluded that, when there is no security mechanism, the SCADA server can be attacked and disabled by a denial-of-service attack. Figure 10 illustrates the SCADA server with the TEVM mechanism, which shows that a lot of resources remained in the system to carry forward other tasks, and indicates that the encrypted authentication mechanism could effectively defend against denial-of-service attacks.



```
top - 19:24:38 up 4 days, 22:00,  3 users,  load average: 4.10, 1.67, 0.69
Tasks: 154 total,   9 running, 143 sleeping,   0 stopped,   2 zombie
%Cpu(s): 48.0 us, 45.4 sy,  0.0 ni,  0.4 id,  0.0 wa,  0.0 hi,  6.2 si,  0.0 st
MiB Mem :   3827.9 total,   2913.7 free,    135.3 used,    778.9 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3422.2 avail Mem
```

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL
IP 172.16.100.233

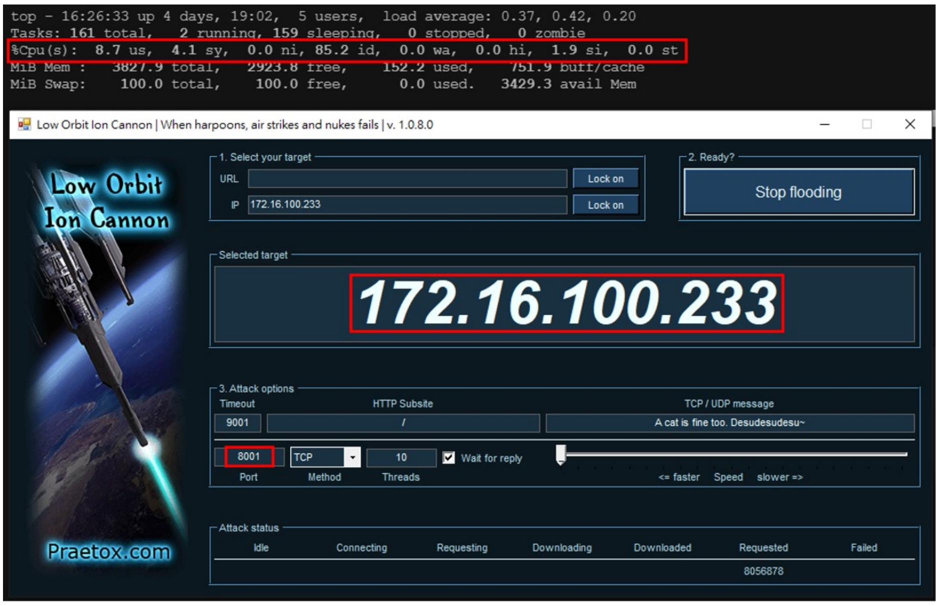
Selected target
172.16.100.233

3. Attack options
Timeout 9001
HTTP Subsite /
TCP / UDP message A cat is fine too. Desudesudesu~
Port 8001
Method TCP
Threads 10
☑ Wait for reply

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					17910018	

Figure 9. SCADA server without TEVM mechanism.



```
top - 16:26:33 up 4 days, 19:02,  5 users,  load average: 0.37, 0.42, 0.20
Tasks: 161 total,   2 running, 159 sleeping,   0 stopped,   0 zombie
%Cpu(s):  8.7 us,  4.1 sy,  0.0 ni, 85.2 id,  0.0 wa,  0.0 hi,  1.9 si,  0.0 st
MiB Mem :   3827.9 total,   2923.8 free,    152.2 used,    751.9 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3429.3 avail Mem
```

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL
IP 172.16.100.233

Selected target
172.16.100.233

3. Attack options
Timeout 9001
HTTP Subsite /
TCP / UDP message A cat is fine too. Desudesudesu~
Port 8001
Method TCP
Threads 10
☑ Wait for reply

Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested 8056878
Failed

Figure 10. SCADA server with TEVM mechanism.

5.3. Performance Analysis

Figure 11 displays the idle situation of the SCADA server's CPU when the SCADA system was running. The X-axis is time in different periods and the Y-axis shows the idle percentage of the SCADA server's CPU. Three lines in different colors show the idle percentage of the CPU under different circumstances: the blue line is under the condition that the SCADA server runs no service, the red line shows how the SCADA server runs to access one temperature and humidity sensor, and the green line is when the SCADA server runs to access one temperature and humidity sensor after adopting the TEVM mechanism proposed in this paper. According to the line graph, while no great difference can be distinguished between the idle server and the server running without employing an encrypted authentication mechanism, the CPU in the server with the TEVM mechanism has been used a little more frequently. Figure 12 presents the assumption that hackers have destroyed the BEMS and controlled it to launch DoS attacks to the SCADA server through LOIC. The X-axis is time in different periods and the Y-axis shows the idle percentage of the SCADA server's CPU. The red line represents the situation when the SCADA server adopted no encrypted authentication, while the blue line represents the SCADA server employing the TEVM mechanism. If no protective mechanism was applied, the SCADA server would be easily disabled by hackers' DoS attacks; however, when the TEVM mechanism was used, DoS attacks were effectively defended.

Figure 13 shows the performance analysis of SCADA server (Control server, CS) accessing a single Internet of Things device. The horizontal axis is the number of times that CS accessed the Internet of Things device, while the vertical axis is the time spent on such access. The blue bar denotes that no encryption verification mechanism is executed, and the orange bar denotes that the complete encryption and verification mechanism is executed. In the experimental analysis, the average access time without the encryption verification mechanism is 105 ms, and the average access time with the complete encryption and verification mechanism is 186 ms. It can be found that the time consumed by executing the complete encryption and verification mechanism is about 1.7 times that of no encryption verification mechanism. However, from the data point of view, it takes a lot of time. In fact, the time consumed in both cases is very short. In addition, in practice, the SCADA system does not have too strict requirements regarding the access time of most Internet of Things devices. Furthermore, we learned from the system integrator that the average time from transmission to response must be controlled within 1 s when integrating this mechanism. Adding to this, according to expert's recommendation, it only requires that a reply is received from Internet of Things devices within 1–2 s. Therefore, the mechanism proposed in this paper is efficient and in line with the demand in the actual field.

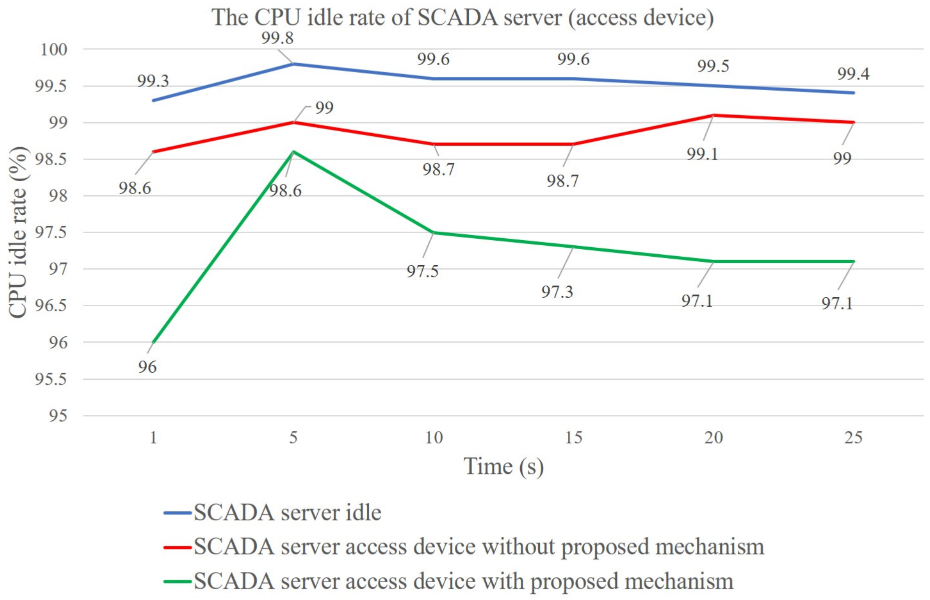


Figure 11. Performance comparison without DoS attack.

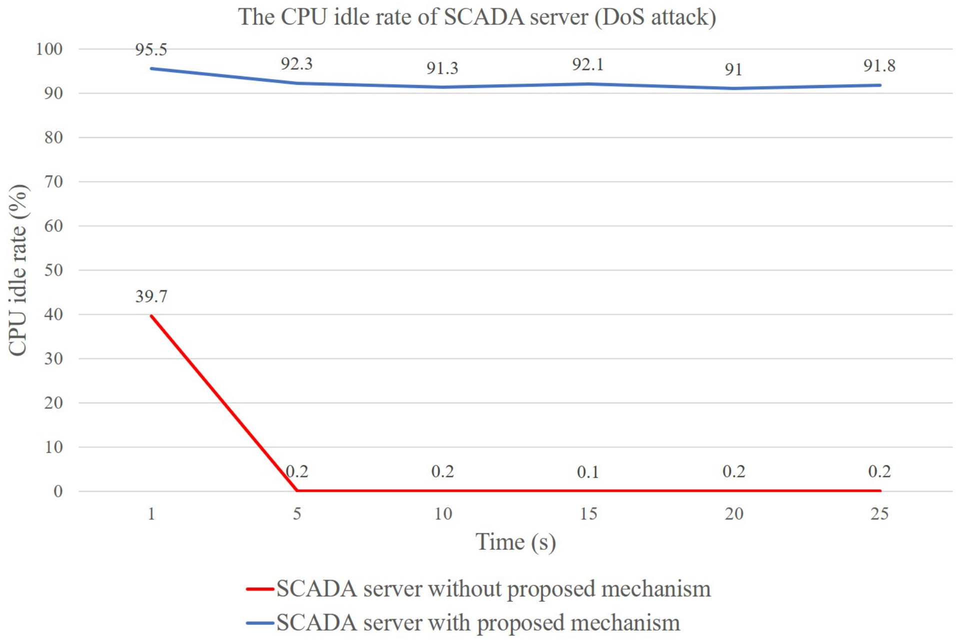


Figure 12. Performance comparison with DoS attack.

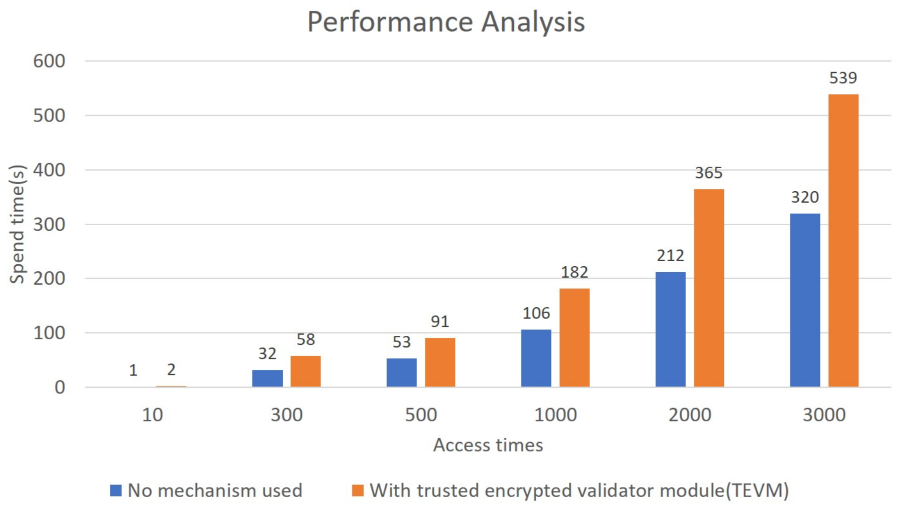


Figure 13. The performance analysis of TEVM.

6. Conclusions

This paper puts forward a module to prevent attackers from performing distributed denial-of-service (DDoS) attacks and a transport layer security (TLS) protocol with an encrypted token identity authentication module to ensure the internet security of SCADA in the IIoT energy management system. This two-way identity authentication process was available through the tokens, devices, and remote control of the server. In addition, as tokens are highly private and the identity information of IoT devices is confidential, this feature could help protect sensitive materials from disclosure. As it requires every entity to run authentication procedures before accessing the network information, the mechanism proposed in this paper could protect industrial networks from external threats. Moreover, in addition to this mechanism defending against DoS attacks, it can also defend against man-in-the-middle, replay, and impersonation attacks. After applying and verifying the mechanism in the energy management system of a Smart Green Energy Science City in southern Taiwan, the experimental results also showed that this mechanism could effectively improve security and was compatible with the real field system. Furthermore, the hardware used in this mechanism was of low cost, which indicates that the mechanism could be applied in reality on a large scale.

Author Contributions: Conceptualization and methodology, Y.-S.Y., S.-H.L. and W.-C.C.; Formal analysis, S.-H.L. and W.-C.C., Supervision, C.-S.Y., Y.-M.H. and T.-W.H., Project administration, S.-H.L. and C.-S.Y., Writing—original draft preparation, S.-H.L.; Writing—review and editing, S.-H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been partially supported by the Ministry of Science and Technology of Taiwan (under grants No. 110-2221-E-006 -038).

Acknowledgments: The authors would like to thank Editor-in-Chief, Editor and anonymous Reviewers for their valuable reviews.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Boyer, S.A. *Supervisory Control and Data Acquisition*, 4th ed.; International Society of Automation: Research Triangle Park, NC, USA, 2009.
2. Webb, J.W.; Reis, R.A. *Programmable Logic Controllers Principles and Applications*, 5th ed.; Phi Learning Private Limited: Delhi, India, 2002.
3. Bobat, A.; Gezgin, T.; Aslan, H. The SCADA system applications in management of Yuvacik Dam and Reservoir. *Desalin. Water Treat.* **2015**, *54*, 2108–2119.
4. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
5. Miśkowicz, M. Unfairness of Random Access with Collision Avoidance in Industrial Internet of Things Networks. *Sensors* **2021**, *21*, 7135. https://doi.org/10.3390/s21217135
6. Parras, J.; Zazo, S. Repeated Game Analysis of a CSMA/CA Network under a Backoff Attack. *Sensors* **2019**, *19*, 5393. https://doi.org/10.3390/s19245393
7. Khan, F.; Rehman, Au, Yahya, A.; Jan M.A.; Chuma, J.; Tan, Z.; Hussain, K. A Quality of Service-Aware Secured Communication Scheme for Internet of Things-Based Networks. *Sensors* **2019**, *19*, 4321. https://doi.org/10.3390/s19194321
8. Kambourakis, G.; Kolias, C.; Stavrou, A. The Mirai botnet and the IoT Zombie Armies. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 December 2017; pp. 267–272, doi:10.1109/MILCOM.2017.8170867.
9. Francino, ; P.N.; Huff, C. Energy Management System. US Patent 9,335,748, 2016.
10. Miwa, K. Building Energy Management System.US Patent 7,797,084, 2016.
11. Rotger-Griful, S.; Welling, U.; Jacobsen, R.H. Implementation of a building energy management system for residential demand response. *Microprocess. Microsyst.* **2017**, *55*, 100–110.
12. Mantravadi, S.; Schnyder, R.; Møller, C.; Brunoe, T.D. Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0. IEEE Access **2020**, *8*, 200305–200321, doi:10.1109/ACCESS.2020.3035963.
13. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019 19**, 1141. https://doi.org/10.3390/s19051141
14. Lu, D.; Han, R.; Shen, Y.; Dong, X.; Ma, J.; Du, X.; Guizani, M. xTSeH: A Trusted Platform Module Sharing Scheme Towards Smart IoT-eHealth Devices. *IEEE J. Sel. Areas Commun.* **2021**, *39*, *2*, 370–383, doi:10.1109/JSAC.2020.3020658.
15. Idriss, T.A.; Idriss, H.A.; Bayoumi, M.A. A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices. *IEEE Access* **2021** *9*, 80546–80558, doi:10.1109/ACCESS.2021.3084903.
16. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. Available online: https://tools.ietf.org/html/rfc8446 (accessed on 1 April 2021).
17. Pricop, E.; Fattahi, J.; Parashiv, N.; Zamfir, F.; Ghayoula, E. Method for authentication of sensors connected on modbus tcp. In Proceedings of the 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, Spain, 5–7 April 2017; pp. 679–683.
18. Garg, S.; Kaur, K.; Kaddoum, G.; Choo, K.R. Toward Secure and Provable Authentication for Internet of Things: Realizing Industry 4.0. *IEEE Internet Things J.* **2020** *7*, *5*, 4598–4606, doi:10.1109/JIOT.2019.2942271.
19. Garg, S.; Kaur, K.; Kaddoum, G.; Rodrigues, J.J.P.C.; Guizani, M. Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. *IEEE Trans. Ind. Informatics* **2020**, *16*, 3548–3557, doi:10.1109/TII.2019.2944880.
20. Choudhary, K.; Gaba, G.S.; Butun, I.; Kumar, P. MAKE-IT—A Lightweight Mutual Authentication and Key Exchange Protocol for Industrial Internet of Things. *Sensors* **2020**, *20*, 5166.
21. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Trans. Ind. Informatics* **2021**, *17*, *5*, 2985–2996, doi:10.1109/TII.2020.3023507
22. Stute, M.; Agarwal, P.; Kumar, A.; Asadi, A.; Hollick, M. LIDOR: A Lightweight DoS-Resilient Communication Protocol for Safety-Critical IoT Systems. *IEEE Internet Things J.* **2020**, *7*, *8*, 6802–6816, doi:10.1109/JIOT.2020.2985044.
23. Borgiani, V.; Moratori, P.; Kazienko, J.F.; Tubino, E.R.R.; Quincozes, S.E. Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks Within Industrial Internet of Things. *IEEE Internet Things J.* **2021**, *8*, *6*, 4569–4578, doi:10.1109/JIOT.2020.3028652.
24. Tajalli, S.Z.; Mardaneh, M.; Fard, E.T.; Izadian, A.; Fard, A.K.; Dabbaghjamanesh, M.; Niknam, T. DoS-Resilient Distributed Optimal Scheduling in a Fog Supporting IIoT-Based Smart Microgrid. *IEEE Trans. Ind. Appl.* **2020**, *56*, *3*, 2968–2977, doi:10.1109/TIA.2020.2979677.
25. Ghosh, S.; Sampalli, S. A Survey of Security in SCADA Networks: Current Issues and Future Challenges. *IEEE Access* **2019**, *7*, 135812–135831.
26. Lyu, C.; Zhang, X.; Liu, Z.; Chi, C. Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks. *IEEE Access*, **2019**, *7*, 31068–31082, 2019, doi:10.1109/ACCESS.2019.2902843.
27. Ghahramani, M.; Javidan, R.; Shojafar, M.; Taheri, R.; Alazab, M.; Tafazolli, R. RSS: An Energy-Efficient Approach for Securing IoT Service Protocols Against the DoS Attack. *IEEE Internet Things J.* **2021**, *8*, *5*, 3619–3635, doi:10.1109/JIOT.2020.3023102.

28. Dammak, MBoudia, RRMMessous, MASenouci, SMGransart, C. Token- based lightweight authentication to secure iot networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4.
29. HULK. Available online: https://github.com/grafov/hulk (accessed on 4 January 2022).
30. Slowloris. Available online: https://github.com/gkbrk/slowloris (accessed on 4 January 2022).
31. Shorey, T.; Subbaiah, D.; Goyal, A.; Sakxena, A.; Mishra, A.K. Performance Comparison and Analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 19–22 September 2018; pp. 318–322, doi:10.1109/ICACCI.2018.8554590.
32. Fadhlillah A.; Karna N.; Irawan, A. IDS Performance Analysis using Anomaly-based Detection Method for DOS Attack. In Proceedings of the 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Bali, Indonesia, 27–28 January 2021; pp. 18–22, doi:10.1109/IoTaIS50849.2021.9359719.
33. Nxumalo, ZCTarwireyi, PAdigun, M.O. Towards privacy with tokenization as a service. In Proceedings of the 2014 IEEE 6th International Conference on Adaptive Science and Technology (ICAST), Ota, Nigeria, 29–31 October 2014; pp. 1–6.