Sensors and Materials, Vol. 33, No. 4 (2021) 1257–1272
MYU Tokyo

S & M 2532

Strengthening Existing Internet of Things System Security: Case Study of Improved Security Structure in Smart Health

Chih-Wei Chang* and Wei-Hsi Hung

Department of Management Information Systems, National Chengchi University,
64, Sec. 2, Zhi-Nan Road, Taipei 116, Taiwan

(Received September 6, 2020; accepted February 9, 2021)

Keywords: Internet of things, IoT security, cybersecurity, Internet of health things, smart health

Sensor applications and Internet of Things (IoT) technology using many sensors and smart devices (IoT devices) have been commercially implemented and are significantly changing our daily lives. However, most IoT devices are vulnerable due to low power consumption and have inadequate physical security protection mechanisms. The information security protection of existing sensors is very limited, particularly when large numbers of smart devices are deployed in smart application systems. This limited protection is a major information security concern and has become an important personal privacy issue. The study of the IoT architecture and security taxonomy in the beginning of this paper will help readers understand our proposed concept for improving the security level of existing systems without taking down the whole deployed system, which is the key contribution of this article. Through an actual case study, we have found that by improving the network planning and security management mechanism and applying network segmentation, monitoring, filtering, and IoT trust connection, we can strengthen the security protection of existing IoT systems. We demonstrated that raising the security level of existing smart health systems will increase market value both now and in the future, and ad hoc IoT security solutions can be feasibly deployed in all sensor application fields.

1. Introduction

In April 2018, the National Health Service (NHS) of the United Kingdom was plagued by the WannaCry ransomware, which not only hampered its emergency care system and instantly forced patients to be transferred due to system failure, but also disrupted over 19000 appointments in one week. This incident shows that once smart devices or IoT systems are hacked, the consequences can be dire. Therefore, we need take the safety of IoT solutions seriously and reduce threats to cybersecurity. We need to ensure sufficient IoT information security and protection capability to ensure that systems can function continuously and achieve their purposes and expected benefits.

Breakthroughs in semiconductor manufacturing, communication technology, and cloud computing as well as artificial intelligence technologies have led to the development of

*Corresponding author: e-mail: 107356509@nccu.edu.tw
https://doi.org/10.18494/SAM.2021.3163

ISSN 0914-4935

lightweight, small-form-factor, and smart devices. IoT technology has become a significant field of research. IoT systems integrate various sensors, monitors, control components, and smart devices, and are connected via wireless sensor networks (WSNs), the Internet, and cloud services. IoT applications have been extensively used and have potential use in a wide variety of fields, such as healthcare, smart homes, smart cities, smart factories, transportation, and government projects.

However, the new technology deploys a plethora of intelligent devices, resulting in a potential threat due to the vulnerability of IoT information security. While there is growing attention on the topic of IoT and security, i.e., the nature of the components and computational capabilities of IoT devices, the variety of communications methods and the complex integration architecture of software interfaces have created more difficulties for managing security in IoT environments. Because of resource constraints and the complexity of environments, IoT devices suffer more serious security challenges than other fields.[(1)] Recently, some scholars have begun studying IoT information security with a threat taxonomy, and others have highlighted the necessity of information security defense measures for IoT systems. However, it is not easy to integrate new components into some existing systems, and information systems for industrial production processes cannot be rapidly updated.[(2)] IoT systems that have already been deployed and started operation are facing complicated security challenges. Meanwhile, past studies have not addressed the improvement of the security protection mechanism of IoT systems in current operation. Thus, how to prevent hacker attacks of such systems is the focus of our research. A critical issue is how to keep existing IoT systems running while upgrading their information security protection capability and ensuring their robustness to new cybersecurity threats.

In this paper, we first review the established research on the application architecture and information security taxonomy of the IoT. In addition, we perform a case study on a reengineering project of an ongoing operation in the smart health domain. The case study explores network planning, network gateway design, and strengthening information security management to achieve the goal of upgrading existing information security protection capabilities without changing all the deployed sensors and smart devices and the software of the IoT system. The reengineering project provides an efficient method for the future security enhancement and deployment of IoT systems.

2. IoT Framework

IoT refers to heterogeneously integrated systems with diverse applications. Researchers must first understand the nature and architecture of IoT solutions in order to propose the most appropriate method of minimizing threats to the cybersecurity of IoT systems. This section first outlines the characteristics of IoT systems, their areas of application, and the system architecture.

2.1 Synopsis of IoT

The concept of IoT is the enhancement of existing communications technology via the Internet to enable human–things and things–things communication.[(3)] Intrinsically, the purpose

of the Internet is to satisfy the need for communication between humans. IoT solutions render a cascade of endpoint components, sensory devices, and digital controllers to adopt a new communications protocol, and such evolution contributes to the alignment of the Internet with data transmission tools that allow machines to directly connect with machines, toward achieving cloud computing. Smart devices and equipment can directly use the Internet to exchange data. Therefore, not only can IoT devices provide real-time data to relevant operators, but the devices can also exchange data, a mode of direct communication also known as machine-to-machine (M2M) communication, to achieve the goal of automated, collaborative operation, thus increasing the degree of system automation and optimizing the operation process.

Smart devices in IoT systems are also called "things", a word used to refer to all sorts of components such as sensors and actuators including pulse sensors, vital signs monitors, digital multimeters, thermostat sensors, controllers, and other endpoint devices. The devices have IP communication protocol capabilities and can use the Internet to conduct data transfer and information exchange.[4] In contrast, the IoT itself refers to heterogeneous integrated network systems that do not require human intervention to connect to physical equipment and virtual systems, such as sensors, embedded electronic systems, software systems, and smart devices, by automatically conducting data exchange through the Internet, generating even more value for users of digital applications.[5]

2.2 Areas of IoT applications

When sensors are combined with automated operation processing and the analysis capabilities of big data, artificial intelligence applications become the smart devices of IoT systems that have auto-feedback capabilities, providing real-time information of the selected on-site environment. Additionally, these smart things with integrated back-end software application systems conducive to IoT systems can provide businesses with multiple potentials for application development, the optimization of existing operation procedures, and increased market value. Multiple IoT applications have led to the recent widespread application of IoT in a wide range of smart service domains. Scholars have categorized IoT application domains into general classifications including traffic control and transportation, logistics management, healthcare, remote healthcare, education, personal and social applications, and intelligent application services. Examples of specific applications include smart factories, advanced planning systems, rural medical care, smart living environment control, smart grids, smart cities, intelligent workplaces, and smart homes.[1,2,5,6–12] Recently, researchers have categorized new IoT cloud platforms into nine domains and 46 service applications,[13] indicating that IoT technology already has the potential for widespread adoption.

2.3 Architecture of IoT

IoT refers to complex heterogeneous networks and application systems. Various researchers have proposed approaches to facilitate the integration of different components, devices, communications functions, software interfaces, and application systems for functionality and

manageability into IoT architectures. IoT architectures can be categorized into three primary layers: the perception layer, the network layer, and the application layer. The interconnection architecture of each layer is illustrated in Fig. 1.[14,15]

The purpose of the perception layer is to use sensory components to collect the status and obtain data from the operating environment, then conduct signal processing and transmit the collected data to local or nearby points for aggregation at another IoT node for subsequent operational processing. The main purpose of the network layer is to enable IoT equipment to conduct data exchange. The designed structure supports communications functions among different near-end smart devices, is equipped with IP networking functions to provide the data transfer capability to IoT equipment at different locations, and is able to connect to the whole back-end system and a cloud platform. The application layer provides users with a platform to view, manipulate, and manage the whole system, capturing the essential spirit of IoT solutions.[6,16–18]

3. IoT Security Analysis

3.1 IoT information security threats

Ukraine was hit by a cyberattack against its power grid system on Christmas Eve in 2015, leaving more than 250000 people without power during a freezing winter. In April 2018, the United Kingdom NHS system was plagued by the WannaCry ransomware.[19] Thus, we need sufficient IoT information security and protection capability to ensure that systems can function continuously and achieve their purposes and expected benefits.

In recent years, most implementations of IoT systems have not considered newly arising information security threats. This is attributed to the rapid pace of IoT deployment in various application services without acknowledging the lack of computational power and protective

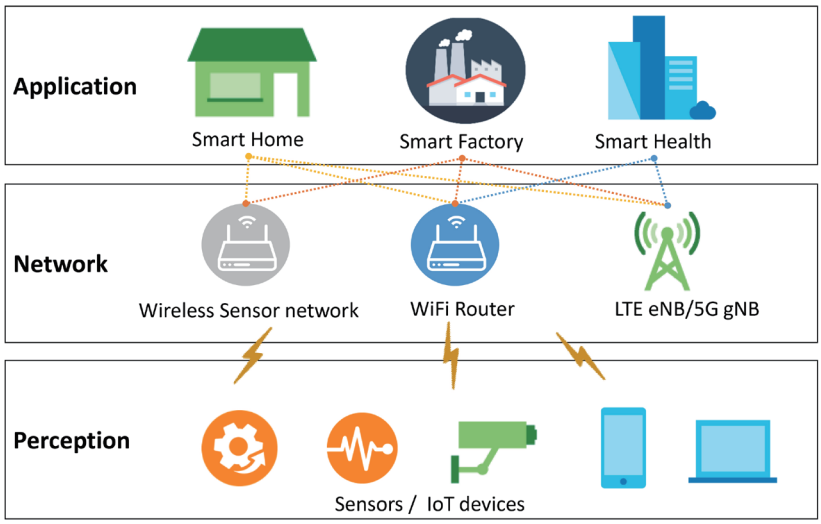

Fig. 1. (Color online) Network architecture of IoT.

mechanisms in most sensor components and smart devices. As a result, IoT devices and software systems exposed to the Internet face serious cybersecurity risks and potential privacy breaches owing to insufficient security protection.[19–23] For example, in the domain of factory control applications, erroneous systems data and control commands will jeopardize the normal operations of critical system infrastructure. In the medical services domain, erroneous sensory data will endanger personal safety, and unauthorized user behavior could cause harm using sensitive information and threaten the privacy of relevant personnel. Therefore, it is clear that if the problems of IoT information security are not addressed, the future development of IoT applications will be precarious and severely undermined.

3.2 Information security

Regarding the security issues concerning information and networking systems, we extract and categorize several characteristics of information security that can serve as principles for planning and establishing IoT information security issues, as an IoT system is also part of the information communications system.[1,24–26] The information security characteristics are categorized into the following:

- Confidentiality: guaranteeing the privacy of the transmission and storage of information; preventing unauthorized personnel from accessing the contents.
- Integrity: ensuring that data cannot be modified by a third party; securing the integrity of data during transmission and storage processes.
- Availability: ensuring that legal users can access system services at any time.
- Authentication: authenticating equipment or user identity, and verifying the identity of sources transmitting data.
- Non-repudiation: guaranteeing that a transmitter cannot deny that they transmitted the information at a later date.
- Privacy: ensuring that a user or account identity cannot be identified, and that users of systems cannot be identified or tracked from their executions and actions.

However, IoT security issues primarily originate from devices. Most smart devices of IoT systems do not have information security functions, making it difficult to manage a large number of IoT devices. IoT devices require only a connection to the Internet to conduct communications with other equipment and software systems. Hence, hackers can attack them at any time.[27,28] Therefore, businesses and organizations using IoT devices need to plan effective protection measures to ensure the continuous, active, and automated operation of their IoT systems.

3.3 Taxonomy of IoT security

To provide the necessary information security defense capabilities for IoT systems, we need to consider all possible information security threats and build a standardized IoT security taxonomy, which will assist researchers in identifying security leaks and operational risks of IoT more clearly, and thus develop a better-planned mechanism for system protection. Therefore,

we consulted previous studies and proposed a taxonomy for IoT information security criteria, as illustrated in Fig. 2.[1,6,29,30]

Sensor applications and IoT technology have been deployed in many fields. Several primary security technologies can be identified, including authentication, authorization, exhaustion of resources, policy enforcement, and trust management. These fundamental elements have been applied in application systems for information security protection.

In terms of the IoT architecture, no model is universally applicable to all IoT application settings as the whole structure is heterogeneous and complex. Notwithstanding, the IoT architecture can still use various information security defense technologies for a comprehensive upgrade of system-wide information security and protection capabilities, including the identification of devices, equipment, and personal identities; authentication; authorization; and secure middleware.[1,6,20,24,30,31]

The communication functions require communications capability to be provided for smart devices as well as information exchange capability between subsystems of equipment at all levels. In terms of communications security protection, functions and technologies that have to be taken into account include the prevention of man-in-the-middle attacks, ensuring data transmission security, and lowering the risks of logging and eavesdropping. We can establish secure communication channels, network access control, and other management mechanisms paired with intrusion detection and prevention (IDP) technology to detect and monitor the network security status. Alternatively, we can use new software-defined networking (SDN) technology to construct a new secure communications environment and achieve secure data communication and storage.[6,29–31]

Protecting data confidentiality and the content privacy protection of operation procedures are critical issues being discussed in information security. Therefore, how to maintain content confidentiality from the viewpoint of IoT data security must be considered. Adopting privacy protection technology and data encryption technology is a conventional approach. Similarly,

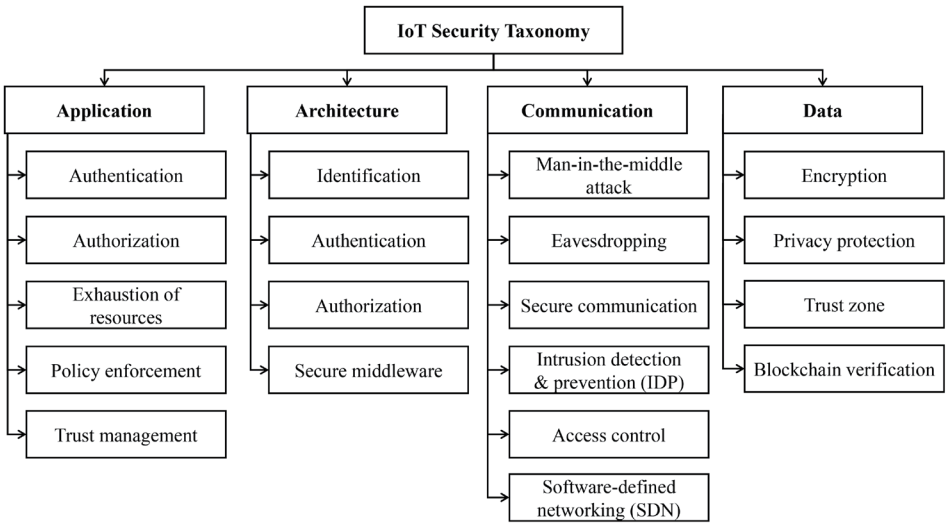

Fig. 2. IoT security taxonomy.

establishing trust mechanisms between different modules, personnel, and equipment within an IoT system is another protective measure. There is also new blockchain technology, which not only provides a data non-repudiation feature but also integrates smart contracts to directly facilitate negotiation with the components of the perception layer and increase the automation of system services.[1,30,32]

3.4 Defense methods in IoT security

In this section, we discuss various IoT information security threats in terms of the specific information security needs of the three layers of the IoT architecture. Information security application technologies proposed by earlier researchers are first addressed. Table 1 presents the various characteristics, solutions, and application technologies of information security needs.

Firstly, the perception layer of the IoT architecture is primarily concerned with obtaining, gathering, and processing actual data on-site. Once the sensory nodes are attacked or damaged, the entire IoT system becomes unreliable. However, a major security risk in IoT also originates from perception-layer devices with insufficient defense capabilities. If the protection of smart devices can be enforced, the weakest point in the IoT system in terms of the threat to

Table 1
Information security characteristics and corresponding solutions.

Characteristics of cybersecurity	Solutions of information security	Application technology and examples
Confidentiality	Messaging encryption, Login encryption, ID and device verification, Authorization management, WiFi channel encryption, VPN (virtual private network), Secure communications protocol	Symmetric encryption: AES, CBC, 3DES Asymmetric encryption: RSA, DSA, ABE VPN: IPSec, SSL, L2TP Encryption protocol: SSH, IKE, TLS, DTLS
Integrity	Hash function, Key management, Digital signature, Trust management	Hash function: MD5, SHA-2, SHA256 Key management: public key infrastructure Digital signature: message authentication code, DSA (digital signature algorithm), RSA, TPM (trust platform module)
Availability	Network access control, Firewall, IDP, Secure gateway, Secure middleware	Firewall: Stateful inspection firewall, Packet filtering firewall IDP: Network intrusion detection system, Host-based intrusion detection system, Perimeter intrusion detection system, SOA (service-oriented architecture)
Identification	ID and device authentication, Authorization management, White list management, Message authentication code, Hash chain	Authorization: IdM (identity management) Message authentication code: HMAC, CBC-MAC, ECDSA, White list: ACL (access control list)
Non-repudiation	Digital signature, Blockchain, RSA encryption	Digital signature: ECDSA, HMAC
Privacy	Pseudonymity, Anonymous communication, Unlinkability, VPN, Trust management, Blockchain	DAA (direct anonymous attestation), EPID (enhanced privacy ID), K-anonymity model, ZKP (zero knowledge proof), Pedersen commitment, IPSec VPN, SSL VPN, L2TP tunnel, Blockchain

information security can be effectively monitored and filtered. According to prior work on security protection for perception-level devices, the perception level of IoT must use devices and communication equipment with authentication and network access control capabilities to prevent unauthorized equipment from entering the network system.[7,17,25,30,31,33,34] At the same time, it is necessary to use secure encryption transmission channels and secure mediation gateways to protect the safety of the communication of exchanged data and to control nodal communications safety. Finally, cryptographic mechanisms and key management must be integrated to dramatically increase the confidentiality of transmitted contents and raise the confidentiality and integrity of point-to-point information exchange.

Secondly, the network layer provides access network and core network functions, adopting the network as the vehicle to provide IoT devices with near-end communications and an inter-layer transmission function at different locations. Applicable technologies proposed by previous researchers have provided information security protection capabilities including encryption wireless channels, authentication mechanisms, authorization management, and isolation subnets.[17,25,33] The core network is used to provide cross-site and cross-level interconnect functions and transmission communications. It has been suggested that the core network can use authorization mechanisms, network access control, firewalls, intrusion detection systems, secure communications, secure routing protocols, key management, and software-defined networks to increase Internet security and protection capabilities.[11,14,24,26,32,33,35]

Also, the IoT application layer mainly provides users with an interactive interface with the IoT system by supporting various software functions and middleware in various service domains. However, owing to the wide-ranging nature of service domains and the diversity and complexity of the intermediary system, it has been recommended that authentication and authorization management, access control, encryption technology, digital signature, key management, trust mechanisms, data privacy and protection, point-to-point protection, information security policy management, blockchain technologies, and so on, be used at this level. A system planner should focus on an interface framework that can establish the appropriate information security and protection measures for each application service system.[1,7,13,17,25,27,31–33,35]

3.5 Security management of IoT

Organizations seeking to protect IoT devices from attack must also address information security management, monitoring, and defensive measures to achieve the goal of continuous system operability.[9] Businesses should review all deployed devices and system equipment within the system environment, and at the same time, isolate network access control from services to prevent unauthorized equipment and anomalous connection behaviors. When certain equipment is under information security attack, measures must be taken to avoid the rapid spread of fallout that may impact standard equipment and other information systems. Secondly, businesses should monitor the operational situation of their IoT system and identify suspicious security threats from event logs, network traffic analysis, and IDP technology, and even renew their information security management policy and raise defense capabilities. In the case of

an information security threat alert, businesses must react concurrently and terminate the attack to achieve their defense objective. Substantially, there must be more effort to strengthen information security, and a goal of management policy should be to raise future defensive capabilities of the IoT system after such an event.

4. Practical Study of IoT Security

4.1 Case study

The case study considered is an IoT application service system operating in the field of smart health. Smart things applied in a vital information console (VIC), a clinical cart, or a physiologic monitor are integrated and connected with a smart ward and a nursing station application system. Each nursing station subsystem is also instantaneously linked to the back-end system to integrate it with a nursing informatic system (NIS) and an electronic health record (EHR). In response to the high risk of an information security threat, the system director urgently requires the security of these intelligent facility systems to be improved without changing the existing IoT infrastructure, which has already been installed and is in operation at each station. The director hopes to reduce the risks of future operational disruption by increasing the information security performance via the upgrade of a limited number of components or subsystems.

4.2 Implementation of new and improved information security measures

As this case study requires no change to the existing IoT infrastructure in the information security reinforcement, three information security upgrade stages are planned. The stages are the implementation of a secure IoT networking process, the improvement of the smart application environment, and the strengthening of the information security management policy (Fig. 3). The methods of implementation are described in detail in the following.

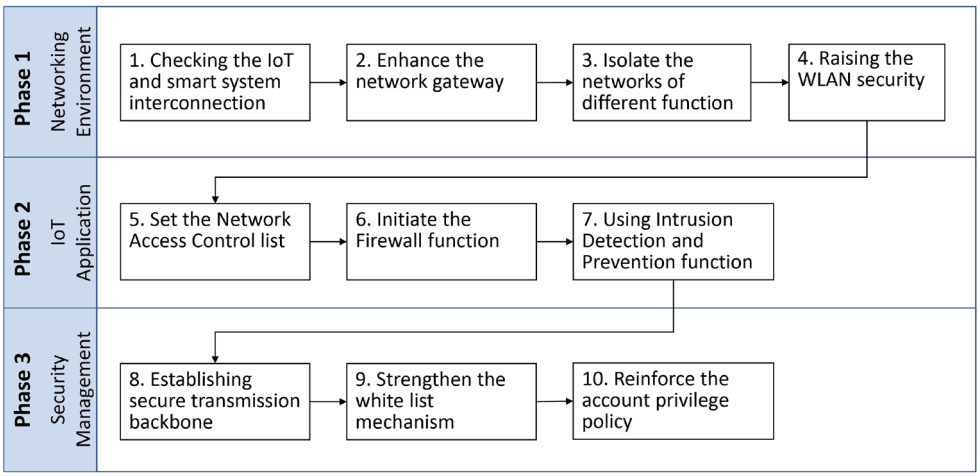

Fig. 3. (Color online) Security improvement flow.

4.2.1 Implementation of secure IoT networking process

Internet communication is one of the key features of an IoT system, which includes near-field IoT device connection and front-end/back-end information exchange via the Internet. Establishing the following policy management rules will effectively ensure networking safety.

(1) Check the interconnections of the IoT devices and smart system
First, the interconnections among the IoT devices and smart system must be identified. All communication requirements and possible intrusion points must be found.

(2) Enhance the intra-gateway network environment
In this case study, a front line of defense is built in the IoT systems in each nursing station by replacing the IoT network gateways with next-generation firewall functions. The new network gateways will help to set up secure IoT communication for smart sensors and application systems.

(3) Isolate networks with different functions
A virtual local area network (VLAN) is used to separate IoT devices and operating management systems with different connections fulfilling different communication requirements, so that the IoT device subnet, managing staff subnet, and public Internet subnet are completely isolated. This approach avoids unnecessary cross-network data exchange, reducing the risk of intrusion for IoT devices and on-site operating computers.

(4) Strengthen the WLAN security
Using the three subnets in (3), different specific service set identifiers (SSIDs) of WiFi local access networks are used to connect different IoT devices, operator mobile devices, or computer and guest terminals. These different WiFi SSIDs can also be connected to specific VLANs to guarantee that the whole network (sensor SSID, managing staff SSID, and public Internet SSID) will perform normal information exchange. A wireless security encryption protocol is also activated to reduce the risks of WiFi internet data transfer theft, man-in-the-middle attacks, and intrusion events.

4.2.2 Improvement of smart application environment

The second stage is the improvement of the smart application environment to enhance security protection and prevent hacking events in each nursing station.

(5) Set network access control list
Although existing IoT devices cannot be modified to include an authentication function, the network access control function of the new IoT network gateway can be used to control permitted devices in each VLAN, which would limit the addresses of a device and access to the IP subnet, and achieve effects comparable to device credential verification.

(6) Initiate the firewall function
Establish a firewall policy on the new network gateways installed in each nursing station to limit the access of the wide area network (WAN) and local area network (LAN) by authorizing limited devices or network addresses, thereby preventing the possibility of hacker intrusion from the Internet and local IoT environment.

(7) Use IDP function

Activating the IDP function on the IoT network gateways of nursing stations can detect abnormal communication packets or signatures of attacks. Once abnormal behaviors in data traffic have been detected, the IoT network gateway can issue a warning message to the system operator, and thus block abnormal traffic to prevent denial of service (DOS) attacks from hackers.

4.2.3 Strengthening of information security management policy

The third stage is to add an authentication mechanism and strengthen security management in the existing software system. In the application layer, the smart application system leads the following management policies to boost the information security protection capabilities without rewriting software for the existing operating application systems or changing the current operational process in each station.

(8) Establishing secure transmission backbone

The newly installed IoT gateways at each station use Internet protocol security (IPsec) to establish virtual private network (VPN) links and connect to the central firewall in the back-end machine room. This achievement builds up a trusted connection, providing the IoT system of each station with a secure data channel for communication with the back-end servers.

(9) Strengthen the white list mechanism

The existing central firewall can be used to control the remote connecting addresses and communications ports of the back-end server system. It can also create white lists that limit access to trusted Internet connections to set up a line of defense for the back-end information system.

(10) Reinforce the account privilege policy

Improving the password strength level and password change frequency of the active directory (AD) can strengthen user password protection and reduce the chance of account/password leaks. Also, the system operator user privilege can be reviewed to minimize account privilege, and each user's access privilege can be limited to access only the specific operating functions required. This will strengthen account and privilege management.

5. Results and Discussion

5.1 Evaluation of IoT security

We use ISA/IEC 62443 as our gold standard to evaluate the security of the new strengthened system in the case study. An evaluation of our approaches to segmentation, monitoring, and strengthening the boundary of the existing system can help increase the reliability and security of the system. Table 2 shows the evaluation of the new implementation based on a seven-point Likert scale questionnaire of the security protection capability. The protection capability of each feature is calculated using the following formula:

Table 2
Information security characteristics and corresponding solutions.

Aspect	Measured feature	Original system	Strengthened system
Application	Identification and authorization	Yes 50% Fulfilled	Enhanced 90% Fulfilled
	Trust mechanism	Required	70% Equipped
System architecture	Device authentication	Required	70% Equipped
	Authorization mechanisms	Required	70% Equipped
	Intrusion detection and prevention	Required	100% Fulfilled
Communications	Secure communications	Required	90% Fulfilled
	Network access control	Required	100% Fulfilled
	Man-in-the-middle attack protection	Required	90% Fulfilled
	Eavesdropping protection	Required	90% Fulfilled
Data security	Trusted connection	Required	70% Equipped
	Privacy protection	Required	70% Equipped

$$P_f = \min \{f_1, f_2, ..., f_n\},$$

where P_f is the protection capability from the measured feature and f_i is a variant factor.

5.2 Improvement of IoT security

A comparison of the original system and the strengthened system in the case study was performed by analyzing the security protection measures of the smart health solution with its IoT information security taxonomy, and the results are illustrated in Table 2. Following reengineering, the system in the case study now has several features at the application level, including three information security protection functions: user authentication, authorization, and the trust mechanism. Structurally, the reengineering mechanism now enables device authentication and IDP. At the communications level, the network environment grants secure transmission via a backbone VPN, along with segregated LAN services, enabling defense against risks such as man-in-the-middle attacks and the logging or eavesdropping of transferred data, as well as network access control management. Finally, regarding data protection, the new system in the case study has a trusted connection environment and a higher level of data privacy.

In the past few years, several researchers have raised concerns about IoT security and provided individual protection features. However, hackers have continued to find the weakest points of information systems simultaneously, and easily damaged the functioning of the whole system. Our case study demonstrates the transformation of cybersecurity, in which a process of an existing IoT system in operation can illustrate useful content covering sensor applications and the enhancement of IoT systems, as discussed in Sect. 4.2 and shown in Fig. 3. This case study was conducted in a smart health environment, where a strengthened security protection mechanism was effectively endowed without replacing the existing sensors, smart things, or application software, in contrast to previous studies. A comparison of the scenarios in this study and previous studies is given in Table 3. The previous studies merely applied an

Table 3
Comparison of proposed security methods between previous studies and present study.

IoT layer	Previous studies		Present study
	Methods proposed only	Methods proposed with verification experiment	Methods proposed and verified methods
Application	authentication,[1,14,20,30,35] authorization,[20,30] privacy solution,[1,30,32,35] security management,[6] secure middleware,[6,24,36] trust platform,[6,24,30,35] access control,[6,24] policy enforcement,[6] key management,[14,31,33–35] encryption[1,25,35]	authentication,[7] forward and backward secrecy[7]	authentication, authorization, trust mechanism, security management, user privilege, firewall policy (white list), secure transmission backbone
Network	DDoS prevention,[24,28] secure communication,[14,24,33,35] access control,[6,14,31,32] eavesdropping,[30] IDP,[1,32] VPN,[32] SDN[1,6,29]	secure localization system at WSN[26]	isolating VLAN, wireless encryption, network access control, firewall, IDP features, VPN, man-in-the-middle attack protection
Perception	data encryption,[17,33,35] device authentication,[12,31] identification[6]	secure localization computing chip,[26] authentication[12]	device authentication by access control list

individual method or performed an experiment to verify results, whereas our study covered several scenarios. We proposed three comprehensive IoT layers and performed a case study to demonstrate that methods of increasing security can be newly deployed in existing IoT systems in operation and also be potentially implemented in other fields.

5.3 Discussion

We proposed a comprehensive IoT solution for improving the security process and protection in an already deployed smart health field and demonstrated the success of the solution. The proposed procedure and solution of this study serve as a good reference model that can further be applied for other cybersecurity purposes, sensor applications, and IoT systems in many fields such as environment control, food and agriculture management, and infrastructure. According to Guo's paper,[2] it is impossible to remove all existing components in a short time in a manufacturing system, making it necessary to reinforce the protection capability while maintaining the existing structure. Our proposed solution has the propensity to be used for IoT and to enhance security management in existing manufacturing fields.

Our proposed method avoids the need to change sensors or IoT devices but requires a device authentication solution via a network mechanism. A possible direction of further research could be to explore security methods for the perception layer and sensor devices in existing IoT systems. Moreover, further investigation of the integration of middleware in the application is desirable.

6. Conclusion

It is difficult for information security protection to achieve non-vulnerability. Instead, the challenge is to achieve the best information security protection level with a limited economic investment. The case study described in this paper aimed to achieve this by minimizing changes to the existing software and hardware infrastructure. The first step was to implement a secure network environment that permits IoT devices and information systems in each nursing station and the back-end server at the center site to function well without hacking. Secondly, a trusted system architecture that integrates access control and a device authentication mechanism was built up. Thirdly, the information security management policy was enhanced by strengthening user privilege management and by establishing a trusted Internet connection that increases security, preventing intruders from hacking the smart application system. The evaluation of the system demonstrated significant success in upgrading every aspect of the information security and defense capability measures of the smart health system, and the case study can be used for reference as a successful model.

For intelligent sensing devices of IoT systems already installed or in operation that cannot be easily or quickly replaced, we recommend implementing a new secure mediation gateway that embeds network access control and next-generation firewall features to achieve local data exchange security and safe remote communication. Additionally, to strengthen information security and management procedures, it is advisable to improve user authentication, device authentication, and operator authorization management at the application systems level. As a result, the privacy of the data can be more securely protected and the likelihood of hacker intrusion into the system can be further reduced.

It is challenging to improve currently operating IoT infrastructure without changing smart devices or running application software; thus, upgrading the security management system in a short timeframe is difficult. Our solution creates the best defense capabilities with minimal system modifications. From this practical and precise study, we have found that the security of IoT is not just a way to adjust hardware and software modules, but it can also be used to enhance information security and protection capabilities from the communications level, system architecture, and management policy. The modification of the networking connections and the authentication of the smart health system provide us with a new defense architecture for IoT systems and information security. We believe that the strengthened information security model proposed in this study provides an agile and highly economical solution to reinforcing the cybersecurity defense capabilities of IoT systems and sensor applications.

References

1 D. E. Kouicem, A. Bouabdallah, and H. Lakhlef: J. Comput. Networks **141** (2018) 1. https://www.sciencedirect.com/science/article/abs/pii/S1389128618301208
2 J. Guo: Sens. Mater. **30** (2018) 1723. https://myukk-org.ssl-xserver.jp/SM2017/sm_pdf/SM1629.pdf
3 J. Tan and S. Koo: Proc. 2014 IEEE Int. Distributed Computing in Sensor Systems (IEEE 2014) 269. https://ieeexplore.ieee.org/abstract/document/6846175
4 O. Uviase and G. Kotonya: (2018) preprint arXiv:1803.04780. https://arxiv.org/abs/1803.04780
5 A. McEwen and H. Cassimally: Designing the Internet of Internet (John Wiley & Sons, United Kingdom, 2013) 1st ed., Chaps. 1–3.

6 D. Das and B. Sharma: J. Comput. Appl. **139** (2016) 23. https://www.researchgate.net/profile/Dolly_Das/publication/301335631_General_Survey_on_Security_Issues_on_Internet_of_Things/links/59e04277aca272386b644f9d/General-Survey-on-Security-Issues-on-Internet-of-Things.pdf
7 C. L. Chen, Y. Y. Deng, C. F. Lee, S. Zhu, Y. J. Chiu, and C. Wu: Sens. Mater. **31** (2019) 1037. https://myukk-org.ssl-xserver.jp/SM2017/sm_pdf/SM1833.pdf
8 B. Chang, H. Tsai, J. Lyu, and T. Yin: Sens. Mater. **31** (2019) 3495. https://myukk.org/SM2017/sm_pdf/SM2026.pdf
9 L. Atzori, A. Iera, and G. Morabito: Comput. Networks **54** (2010) 1. https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf
10 L. Tan and N. Wang: Proc. 2010 3rd Int. Conf. Advanced Computer Theory and Engineering (IEEE, 2010). https://ieeexplore.ieee.org/abstract/document/5579543
11 W. Hsu, W. Chen, H. Kuo, Y. Shiau, T. Chem, S. Lai, and W. Fan: Sens. Mater. **32** (2020) 183. https://www.myukk.org/SM2017/sm_pdf/SM2095.pdf
12 B. Ndibanje, K. Kim, Y. J. Kang, H. Kim, T. Y. Kim, and H. J. Lee: Sens. Mater. **29** (2017) 953. https://myukk.org/SM2017/sm_pdf/SM1385.pdf
13 P. Ray: J. King Saud Univ. – Comput. Inf. Sci. **30** (2018) 291. https://www.sciencedirect.com/science/article/pii/S1319157816300799
14 K. Zhao and L. Ge: Proc. 2013 Ninth Int. Conf. Computational Intelligence and Security (IEEE, 2013) 663–667. https://ieeexplore.ieee.org/abstract/document/6746513
15 T. Hsu, Y. Tsai, D. Chang, F. Liu, and C. Chang: Sens. Mater. **31** (2019) 1815. https://myukk.org/SM2017/sm_pdf/SM1901.pdf
16 L. Atzori, A. Iera, G. Morabito, and M. Nitti: J. Comput. Networks **56** (2012) 3594. https://www.sciencedirect.com/science/article/abs/pii/S1389128612002654
17 M. Leo, F. Battisti, M. Carli, and A. Neri: Proc. Euro Med Telco Conf. (IEEE, 2014) 1. https://ieeexplore.ieee.org/abstract/document/6996632
18 B. L. R. Stojkoska and K. V. Trivodaliev: J. Cleaner Prod. **140** (2017) 1454. https://www.sciencedirect.com/science/article/abs/pii/S095965261631589X
19 M. Harkins and A Freed: J. Law Cyber Warfare **6** (2020) 148. http://www.jstor.org/stable/26441292
20 A. Mahmoud, G. Russello, and B. Crispo: J. Inf. Secu. Appl. **38** (2018) 8. https://www.sciencedirect.com/science/article/abs/pii/S2214212617302934
21 D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac: Ad Hoc Networks **10** (2012) 1497. https://www.sciencedirect.com/science/article/abs/pii/S1570870512000674
22 J. Stankovic: IEEE Internet Things J. **1** (2014) 3. http://web.eecs.umich.edu/~prabal/teaching/resources/eecs582/stankovic14iot.pdf
23 C. M. Medaglia and A. Serbanati: An Overview of Privacy and Security Issues in the Internet of Things (Springer, 2019) p. 389. https://link.springer.com/chapter/10.1007/978-1-4419-1674-7_38
24 Internet of Things: Survey on Security and Privacy: https://arxiv.org/pdf/1707.01879.pdf (accessed July 2020).
25 H. Noura: HDR dissertation (University Pierre and Marie Curie, 2016).
26 W. Sung and S. Hsiao: Sens. Mater. **32** (2020) 115. https://myukk.org/SM2017/sm_pdf/SM2090.pdf
27 A. Sfar, E. Natalizo, Y. Challal, and Z. Chtourou: Digital Commun. Networks **4** (2018), 1. https://www.sciencedirect.com/science/article/pii/S2352864817300214
28 T. Chang and C. Hsieh: Sens. Mater. **30** (2018) 857. https://www.myukk.org/SM2017/sm_pdf/SM1544.pdf
29 A. Akhunzada, A. Gani, N. B. Anuar, A. Abdelaziz, M. K. Khan, A. Hayat, and S. U. Khan: J. Network Comput. Appl. **61** (2016) 199. https://www.sciencedirect.com/science/article/abs/pii/S1084804515002842
30 F. Alaba, M. Othmana, I. Hashema, and F. Alotaibib: J. Network Comput. Appl. **88** (2017) 10. https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455
31 B. Ndibanje, H. J. Lee, and S. G. Lee: J. Sens. **14** (2014) 14786. https://www.mdpi.com/1424-8220/14/8/14786
32 R. H. Weber: Comput. Secur. **26** (2010) 23. https://www.sciencedirect.com/science/article/abs/pii/S0267364909001939
33 A. Oracevic, S. Dilek, and S. Ozdemir: Proc. 2017 Int. Symp. Networks, Computers and Communications (IEEE, 2017) 1. https://ieeexplore.ieee.org/abstract/document/8072001
34 E. Borgia: Comput. Commun. **54** (2014) 1. https://www.sciencedirect.com/science/article/abs/pii/S0140366414003168
35 B. Zhang, X. Ma, and Z. Qin: J. Electron. Sci. Technol. **9** (2011) 365. https://academicpublishingplatforms.com/downloads/pdfs/jest/volume1/201202091139_Security_Architecture_on_the_Trusting_Internet_of_Things.pdf
36 M. Yassein, M. Shatnawi, and D. AI-Zoubi: Proc. 2016 IEEE Int. Internet of Things and Pervasive Systems Conf. (IEEE, 2016) 1. https://ieeexplore.ieee.org/abstract/document/7745303

About the Authors

Chih-Wei Chang received his B.S. degree from Soochow University, Taiwan, in 1994 and his M.S. degree from the University of South Australia, Australia, in 2006. From 1995 to 2016, he worked as a system integrator, telecom operator, and network vendor, where he acquired considerable experience in the telecommunications and network integration fields. Since 2016, he has been a technical director at Zyxel Communication. At present, he is a Ph.D. candidate at the Department of Management Information Systems, National Chengchi University. His research interests are in computer networking, IoT, and cybersecurity.

Wei-Hsi Hung received his B.E. degree from Feng Chia University, Taiwan, in 1996 and his M.M.S. and Ph.D. degrees from the University of Waikato, New Zealand, in 2001 and 2006, respectively. From 2007 to 2019, he was an assistant professor and associate professor at National Chung Cheng University and National Chengchi University, Taiwan. Since February 2019, he has been a professor at National Chengchi University. His research interests are in e-commerce, IS alignment, security management, and information systems.