

Article

GDPR Personal Privacy Security Mechanism for Smart Home System

Yun-Yun Jhuang¹, Yu-Hui Yan² and Gwo-Jiun Horng^{2,*} ¹ Department of Management Information Systems, National ChengChi University, Taipei 11605, Taiwan² Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan 71005, Taiwan

* Correspondence: grojium@stust.edu.tw

Abstract: In the era of vigorous development of the Internet of Things (IoT), the IoT has been widely used in people's daily life. Before the user starts using an IoT product, the developer provides a privacy consent form for the user to fill in. However, the content of the consent form is usually too long for the user to read, and the user neglects the provisions related to privacy use, which often results in personal information being recorded in the database of the product without the user's knowledge. To protect users' informed use, we propose a privacy protection standard of the general data protection regulation (GDPR) law applicable to smart-family-related applications and data security with a consensus mechanism. We also propose a unified device data format agreement. Each product can communicate with each other through a smart housekeeper and can collect personal information between its own products and users based on the personal data protection law. Through practice, we demonstrate the feasibility of this open system. In addition, we also collected 70 questionnaires. If the GDPR specification is placed on smart appliances, about 90% of people can accept smart appliances. If smart appliances can be compatible with different brands' unified standards, about 97% of people can accept smart appliances. Therefore, we recommend the introduction of GDPR specifications for smart home appliances.

Keywords: Internet of Things (IoT); EU general data protection regulation (GDPR); consensus mechanism



Citation: Jhuang, Y.-Y.; Yan, Y.-H.; Horng, G.-J. GDPR Personal Privacy Security Mechanism for Smart Home System. *Electronics* **2023**, *12*, 831. <https://doi.org/10.3390/electronics12040831>

Academic Editor: Christos J. Bouras

Received: 7 January 2023

Revised: 1 February 2023

Accepted: 3 February 2023

Published: 7 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the rapid development of science and technology, the application of the IoT has become an indispensable part of people's lives. According to a McKinsey Digital report, its IoT will have a certain impact on the economy by 2025. From the statistics, it can be seen that the total undervalued value is 4 trillion, and the overvalued value is 11 trillion [1]. Its application can range from small to large scale. For small scale, it can be used to understand and control home appliance status from a distance in terms of general household equipment, such as air conditioners, refrigerators, televisions, etc. The large-scale representative is a large-scale factory with extremely high productivity. With the maturity of the IoT, production speed can be improved to increase economic value.

The convenience of the IoT is beyond human imagination. The most common places to use the IoT are factories and cities. With the emergence of many sensors and Radio Frequency Identification (RFID) technology, factories have become the places where the IoT is applied most, leading to the emergence of the term Industry 4.0 [2]. After the sensor technology is combined with the machine and connected to the Internet, the sensor data are transferred into the database, and the data are analyzed in real time so that the production line can be corrected in the shortest time, thus improving production speed. In addition, it can improve product quality and enable employees to efficiently produce customized products [3].

In order to improve the quality of life, many manufacturers have developed smart home appliances. Generally, smart appliances record the user's habits or judge weather

conditions of the day and adjust themselves. For example, the air conditioner will give the most comfortable temperature and wind direction according to the indoor temperature and human body position. However, smart devices are constantly innovating, and they have also developed exclusive applications that can interact with home electronic devices. Some manufacturers have designed a master control system combining artificial intelligence and speech recognition to provide users with voice control to control household appliances.

In real life, the development and practical application of the IoT can connect hundreds of millions of devices [4], indicating the arrival of huge amounts of data, and some of the data are relatively private information, such as username, IP address, time of use, and religious belief. The data generated by IoT devices can be used for a wide range of purposes. The data are likely to be analyzed without the user's knowledge, which can lead to data misuse and victimization of the user.

As a variety of smart home appliances replace traditional home appliances, it simultaneously raises some concerns and has the potential to improve the quality of life of users. Smart home appliances on the market have a variety of contents and services. When users buy products, it means they need to match the applications provided by the manufacturer to interact. Users are constrained by the products designed by the brand, which limits their choices and leads to low use rate of smart home appliances [5]. Users must fill in terms before operating the application. Generally, the consent terms ask users whether they agree to collect personal information. When users choose not to, the application will not operate. Users need to consent to the collection of personal information, which means that personal privacy may be exposed at any time.

Most users in China have not yet understood the personal data collected by devices. To help users understand the details of personal data collection and protect users more simply, this paper joined the most stringent European General Data Protection Regulation (GDPR) in the world, designed the smart home devices in this study to protect users, and paid special attention to the memory block of personal data exposure.

This paper focuses on two key projects, namely, GDPR personal information protection and consensus mechanisms to give users the right to choose their personal information and equipment data generated by smart housekeepers. The goal is to provide users the right to choose their personal information freely. In recent years, GDPR has been the most rigorous data protection law and the focus of attention of all countries, so all countries are following suit. Those who need to enter the EU market must comply with the relevant provisions of the GDPR. In recent years, the cookie consent notice seen by browsing a website is also set according to the GDPR [6]. Because the website may involve the collection of messenger data or tracking the location, users can protect the right to personal sensitive information through this regulation. The consensus mechanism is a technology of memory blockchain, which is one of the most core technologies. It is a mechanism used to ensure that participants reach consensus and achieve trust between blocks through decentralized consensus algorithms. At present, the consensus mechanism is applied in the field of cryptocurrency. Through the consensus mechanism, fairness, efficiency, and consistency can be achieved.

This paper combines the concept of legal protection and consensus mechanisms into IoT technology to implement security management on the data generated by the equipment in the smart butler and the user's personal information data. Through the framework proposed in this paper, users can better understand the personal data processing principles in EU general information protection regulations and their own right of refusal. If users want to remove the device history records stored in the system, they can implement the right of deletion to remove the records.

In this manuscript, we added the GDPR data protection specification to the intelligent butler equipment of the Internet of Things to realize the GDPR data protection specification. In contrast, on the basis of compliance with the principle, GDPR system was not used, the minimum collection volume of GDPR data was kept confidential for the user's personal

data, and GDPR pseudonym protection was supported to make it impossible to meet the requirements.

In addition, the user can decide whether the GDPR rejection right of the recorded data needs to be checked according to the individual. Compared with the existing system, users can have more choices in terms of recording personal data.

Compared with the existing service communication architecture and standards in the smart home industry, the main advantage of this research was to propose a unified device data format protocol. Each product can communicate with each other through a smart housekeeper and can keep the personal information collection between its own product and users based on the personal data protection law. Therefore, the protection of personal information is relatively complete.

This paper contributes to the research literature in four major areas: (1) using the unified device data format protocol, each product can converge and transmit information to each other, and each product can maintain data collection with users; (2) we designed and imported GDPR data protection mechanisms into the smart home appliance IoT platform; (3) we increased the lifetime, interaction, and thoroughness of interest groups; and (4) it promoted people's willingness to use the smart family system to realize these goals.

The framework of this paper is mainly divided into five sections. The first section states the background, motivation, and research purpose of this paper, and it outlines the framework of each chapter. The second section discusses the related literature, including IoT, memory blockchain, and GDPR. Through this section, we can better understand the basic concepts of this paper. The third section is the research method of the paper. It presents the overall architecture of the intelligent butler system in the form of a system diagram and then explains how the equipment created in this design can protect the user's personal resources and how to combine IoT equipment with the consensus mechanism in the memory blockchain. The fourth section presents the experimental process and explains in detail where and how to apply GDPR in this system. The fifth section is the summary, contribution, and suggestions for future research.

2. Related Work

This section introduces the relevant content and technology of this paper, which will facilitate the subsequent system introduction, including the Internet of Things, general data protection regulations, and consensus mechanisms.

2.1. IoT

IoT technology serves to connect various independently operated devices or objects to the Internet [7] and realize interconnection and intercommunication. There are two ways for objects to connect to the network: wired networks or wireless networks. The most common way is to connect to wireless networks. Through wireless network technology, not only can the data obtained by devices can be transmitted to computers or servers, but mobile phones or computers can also be used to connect objects to devices or machines for control. In daily life, IoT technology is mostly used in factories, but in recent years, the application of home IoT has gradually become a trend [8].

In the application of home IoT, the most common smart devices include smart light bulbs, smart switches, sweeping robots, and smart speakers. The difference between smart home appliances and general home appliances lies in whether there is an Internet connection. By using the Internet connection method, users can use mobile phones or computers to control home appliances in other places at any time to achieve a system of interconnection between things. The main concept of IoT technology is information reading and transmission. Reading is to obtain information through sensors, while transmission is to transfer information obtained by sensors through the Internet [9].

The concept of IoT originated in 1970. At that time, the world's first IoT device connected to the Internet was a Coke vending machine [10], which was in the Carnegie Mellon University (CMU) in the United States. It was developed by students of the

Department of Computer Science. It provided functions such as confirming the quantity of beverages in the vending machine and checking the inventory.

According to literature records, the term IoT officially appeared in public in 1999, when it was first proposed by Kevin Ashton of Procter&Gamble (P&G). At first, Kevin Ashton used the title [11,12] in his speech to explain how to apply Radio Frequency Identification (RFID) to the company's supply chain. So far, IoT involves many technologies, such as cloud computing, low-energy wireless communication, and wireless sensor networks, and these technologies are also developing continuously [13].

IoT architecture is generally divided into two types, namely, three-tier architecture and five-tier architecture. The most common is three-tier architecture [14]. The three tiers are the perception layer, network layer, and application layer. IoT devices can be transmitted through wireless networks, mobile networks, Bluetooth, or wired networks [15]. Application layer applications cover everything in human life, such as smart homes that can improve the quality of life, smart agriculture that can monitor the quality of crops, and smart cities that can assist medical personnel in medical care and monitoring traffic conditions [16,17].

2.2. GDPR

GDPR [18,19], jointly formulated by the European Parliament, the European Executive Committee, and the European Council, has 99 articles. It was passed in April 2016 and took effect in May 2018 [20–24], replacing the Data Protection Directive launched by the European Union in 1995. GDPR is a regulation on the protection of personal data and privacy of all EU citizens in EU laws. It is implemented in countries belonging to the EU. All enterprises that have business dealings with EU countries, regardless of their location, also belong to the implementation scope of GDPR.

On 14 April 2016, the European Parliament adopted the GDPR, and the regulation came into force 40 days after it was published in the Official Journal of the European Union on 24 May of the same year [25]. On 25 May 2018, two years after the regulation came into force, the EU regulations directly applied to all Member States. On 20 July of the same year, the Joint Commission of the European Economic Area and Iceland, Liechtenstein, and Norway reached an agreement to comply with the regulation, and GDPR came into effect in the countries of the European Economic Area.

The differences between the national individual capital law and GDPR are shown in Table 1. Within the scope of regulation, it is difficult for the country to prosecute and punish overseas offenders due to its international status. The difference between the requirements of consent is that the country can obtain the consent of the data subject explicitly or implicitly, and GDPR must inform the clear action. A vague description or an option that is preset as consent may violate the GDPR. The right to be forgotten in the home country is notified by the processor to the party concerned that the specific purpose of collecting personal information disappears or the party concerned requests to delete personal information.

In addition to the above circumstances, GDPR also gives the party concerned the right to withdraw its consent. The data portability right has no relevant provisions in the country. GDPR stipulates that the data subject has the right to require the data controller to provide itself or transmit it to other designated controllers. Regarding obligations of data controllers and processors, each country requires that the safekeeping of personal data must take security measures and meet the current technological or professional standards. When GDPR requires large-scale processing of personal data, a data protection impact assessment should be made, and a dedicated data protector should be appointed. In principle, the country allows cross-border transmission of individual assets. Except for special circumstances, GDPR prohibits cross-border transmission of individual assets in principle, except for obtaining sufficient recognition or enterprises meeting the protection measures.

Table 1. Differences between China’s individual capital method and GDPR [26].

Matter	National Personal Capital Law	GDPR
Scope of specification	It is difficult to prosecute foreigners	If we collect personal resources from EU citizens, it will be regulated
Requirements of consent	Can be expressed or implied	Must inform clear action
The right of data subject to be forgotten	The processor shall take the initiative to inform that the specific purpose of personal data collection disappears, or the party concerned requests to delete personal data	Give the parties the right to withdraw their consent
Data portability of data subject’s rights	No relevant regulations	The data subject has the right to require the data controller to provide itself or transmit it to other designated controllers
Obligations of data controllers and processors	Security measures must be taken to keep personal data, and the technology or professional standards at that time must be met	When processing individual resources on a large scale, a data protection impact assessment shall be prepared, and a dedicated data protection officer shall be appointed
Cross-border transmission	Cross-border transmission is allowed and prohibited only under special circumstances	It is only acceptable to obtain sufficient certification or the enterprise complies with the protection measures

2.3. Consensus Mechanism

As one of the core technologies of the memory blockchain [27], the consensus mechanism plays an indispensable role in obtaining protocols in a distributed environment. The consensus mechanism is a combination of consensus and mechanism. The consensus is to agree on different opinions or interests and achieve consistency. The mechanism is a rule. As the memory blockchain is a point-to-point network system, anyone can participate in the network and use the system without a central server to jointly manage the entire system. It is thus necessary to maintain the operation order and fairness of the system by the rules of the consensus mechanism and reward the nodes that provide resources to maintain the memory blockchain and punish the nodes that intend to harm the system.

Most people think that the consensus mechanism is the protocol generated by the memory blockchain, but in fact, the consensus mechanism came out about 20 years earlier than the memory blockchain. The consensus mechanism appeared in 1989. Lynch, Dwork, and Stockmeyer first proposed in 1988 that consensus was the beginning in the case of partial synchronization [28], while the first consensus mechanism was the Paxos algorithm [29] proposed in 1989. Subsequently, the Raft algorithm, Byzantine fault tolerant, and multi-Byzantine protocols were derived. In recent years, with the popularity of memory blockchain cryptocurrencies, many consensus mechanisms suitable for cryptocurrencies have been developed, and each cryptocurrency uses different consensus mechanisms.

At present, there are eight common consensus mechanisms: workload proof [30], holding proof [31], agent holding proof [32], space proof [33], Paxos algorithm, Raft algorithm [34], Byzantine fault tolerance [35], and LibraBFT [36]. None of the eight consensus mechanisms is perfect, and each has its own advantages and disadvantages. Although there is currently no perfect consensus mechanism, there is a concept of cryptocurrency using a hybrid mechanism, which combines workload proof and holding proof to balance their respective shortcomings.

Jingwen Pan et al. compared three main consensus mechanisms in the paper Development in Consensus Protocols: From PoW to PoS to DpoS, which were workload proof, holding proof, and agent holding proof. The author said that newer protocols could solve the problems of previous protocols. For example, proof of holdings and proof of agent holdings could solve the problems of running speed and resource consumption of

proof of workload. The security problem also alleviated 51% of attacks harmful to proof of workload [37]. According to Omar Alfandi et al. in [38], in the context of the IoT and memory blockchains, using Byzantine fault-tolerant consensus protocols to select a group of authenticated devices in the network was considered as a more efficient solution than other consensus protocols. In this paper, the authors evaluated the fault tolerance of different network settings and verified their proposed model. The research results showed that the mixed scenario proposed by the authors was better than the non-mixed scenario.

The Byzantine general problem is a distributed peer-to-peer network communication fault-tolerance problem, which was proposed by Leslie Lamport in 1982. In the paper The Byzantine General Problem, the author discussed how a reliable system should handle the failure of one or more computers, and the computer with failure may often be ignored or send wrong conflict information. The author called these problems Byzantine problems [39].

Considering that the personal information collected in smart appliances and the data generated by smart appliances need to be properly and reasonably operated, this paper combines GDPR to regulate the right to use personal information and device data. The user can clearly know the use of personal information and equipment data through the GDPR specification of the system, and the user can also decide whether to accept the data generated by the system's recording equipment. According to the provisions in the GDPR, users need not worry about whether they need to have the protection of this regulation in a specific country.

With the emergence of a large number of smart home appliances, ensuring the safety of equipment is a difficult and very important task. We investigated how to confirm whether the equipment is under the control of the intentional person. Therefore, among many consensus mechanism technologies, the choice of Byzantine general is the most appropriate. We used the concept of Byzantine general problem to judge whether the equipment is safe based on the consensus reached among the equipment terminals.

3. System Model

Due to the maturity of IoT technology and the increasing number of users, personal digital information and values in the living environment have become indispensable data for IoT technology. The more data are obtained by the IoT, the more convenient life will be. In view of data security, this system was standardized with the most stringent GDPR, and the consensus mechanism technology was used to confirm whether the equipment was controlled by unknown people. This paper hopes to solve users' data security concerns through three different technologies.

The system architecture of this paper is shown in Figure 1, which is composed of three parts: GDPR provisions, equipment data format conversion, and the consensus mechanism. GDPR provisions should be applied to the template system to provide a guarantee for users' personal information. When users add smart home appliances, they can decide whether to record device data according to their preferences. Since there is no uniform data format in the smart home system on the market today, if users want to buy smart home appliances, they must choose the same brand, which indirectly leads to a decline in users' purchasing desire. To solve this problem, the system will convert the data format of household appliances of different brands so that users can choose more smart appliances without being limited to the same brand. The consensus mechanism is used to ensure the security of the user's equipment. The Byzantine general problem using the consensus mechanism can determine whether the equipment is under the control of the user.

In this paper, the system operation module is shown as the schematic diagram of each module in Figure 2, which is divided into four modules: server side, device control side, user control side, and consensus mechanism. The server side is responsible for providing services, the device control side is responsible for converting the device data format and communicating with the server side, and the user control side is responsible for providing the interface for the user to control the device. Then this paper introduces the hardware equipment used by the four modules, the server erected, the transmission

mode, the technology used, the operation mode provided for users, and how to combine the four modules.

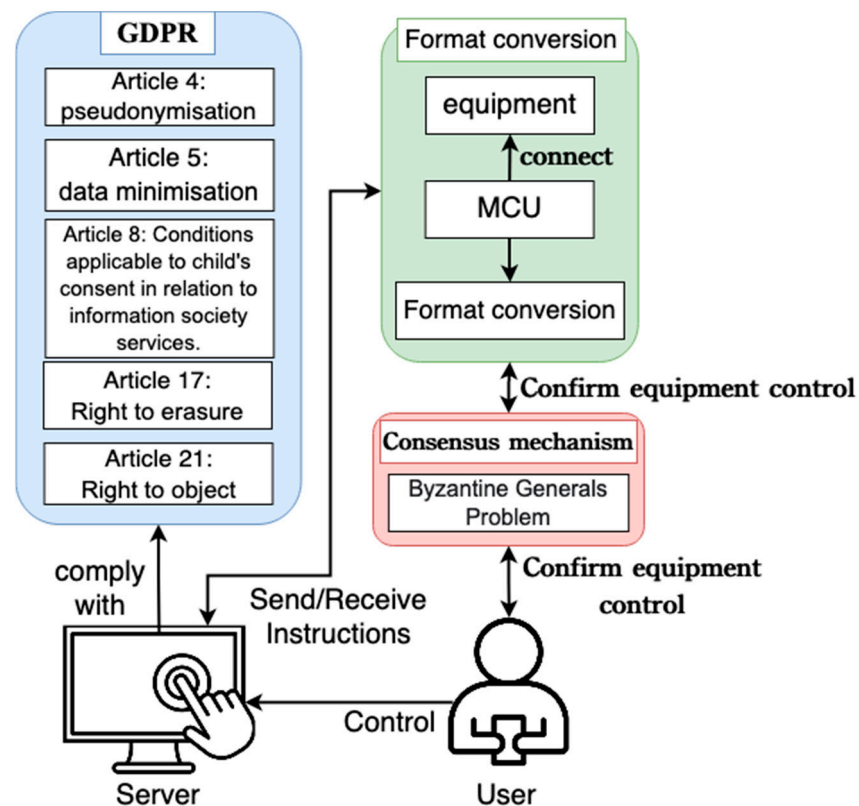


Figure 1. Schematic diagram of system architecture.

The hardware device used on the server side was Raspberry Pi 4, and the socket server, PostgreSQL database, PHP website, and user interface provided for users to operate were set up in Raspberry Pi 4. The socket server also serves an important role as a bridge between the transmission of each module. The device control end and the user control end are connected to the server through the wireless network. The user control end can transmit the instructions to the device control end through the socket and control the household appliances.

The database built on the server side was PostgreSQL, which is an associated database. The database is responsible for storing various data in this system. The data stored include the user account password and the use status of household appliances. The purpose of recording the user account password is to provide users with access to the system, while the purpose of recording the status of household appliances is to provide users with a historical record of the real-time status or status of household appliances.

The server-side user interface is written using Python language graphical interface PyQt, which provides users with a simple operation screen. This service combines GDPR and provides users with six operation functions, including adding users, adding devices, logging off devices, deleting records, viewing device status, and viewing historical records. This paper introduces how to integrate GDPR into each function and the applied provisions in Section 3.2 and describes the provisions in detail.

The main hardware of the device control terminal is the development version of ESP32 single chip microcontroller, which combines Wi-Fi and Bluetooth functions and has a low cost. ESP32 is used to connect with household appliances and convert the data format of the original household appliances to the unified format of the system. ESP32 transmits the converted data to the socket server on the server side through Wi-Fi and stores the home appliance status in the database. The device control end generates a log file and transmits

it to other home appliances and the user control end, and it confirms with the user control end through the consensus mechanism to ensure that the device is controlled by family members. In Section 3.3, this paper introduces how the system uses the technology of the consensus mechanism.

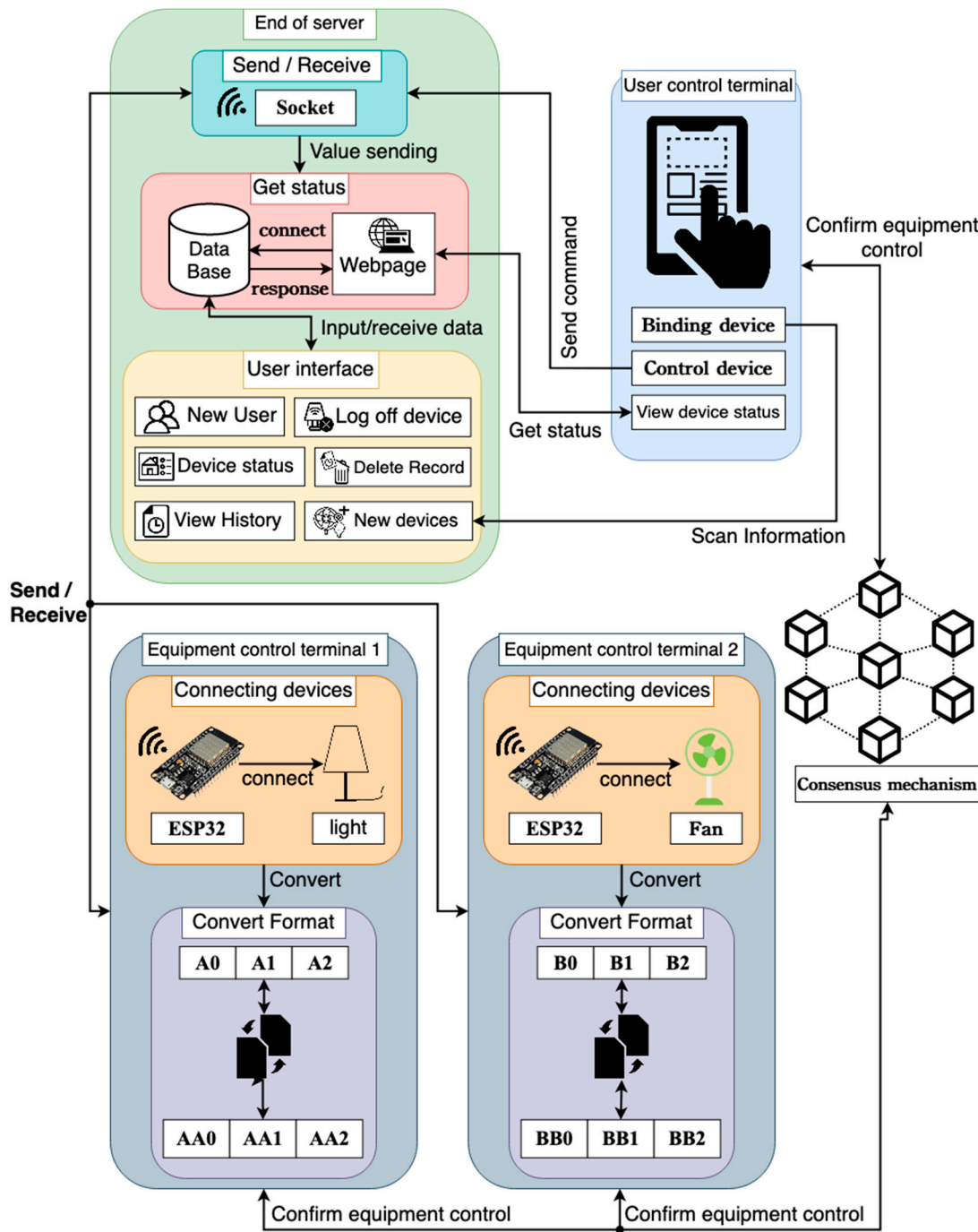


Figure 2. Module connection framework.

The mobile application developed by the user control terminal for this system is written using Flutter suite. The user control terminal is designed with five functions for users to operate, including user login, binding device, controlling device, viewing device status, and logging off. The user login function can only log in to the account that has been applied for on the server to ensure that the user is a family member. The device-binding function scans the QR code generated by the server to bind the device to the APP, and the

control device function controls the device. The view device function allows users to view the current usage status of the device.

3.1. GDPR Articles

GDPR is the largest and most rigorous data protection regulation. Compared with other data protection regulations, the scope of GDPR is not only limited to specific regions but also to the people or companies of any country. The systems generated by European companies and the software and hardware that European people will use are subject to the scope of GDPR. This paper used five GDPR provisions to provide users with a secure system environment.

The GDPR provisions used in this system are shown in Table 2. Item 5 pseudonymization in the definition of Article 4 refers to the mechanism of processing personal data. Without the use of additional information, personal information cannot be identified, provided that the additional information is kept separately and subject to the constraints of science, technology, and organizations to ensure that the personal information cannot identify the person concerned. The system complies with this provision and changes the identifiable name to the name filled in by the user's preference so that the information of the party concerned cannot be identified.

Table 2. Explanation of GDPR Articles [40].

Article No	Article Name	Article Description
Article 4 Item 5	Pseudonymization	It means that personal information cannot be identified without using additional information.
Article 5 Point c of Item 1	Principle of minimum data collection	Personal data should be appropriate, relevant, and limited to the minimization of necessary data related to processing purposes.
Article 8	Conditions applicable to child's consent in relation to information society services	It is legal to process the personal information of children over the age of 16, but it is legal only with the consent and authorization of the legal guardian if they are under the age of 16.
Article 17	Right to be forgotten	The data party shall have the right to delete personal information from the controller without unreasonable delay, and the controller shall have the obligation to delete personal information.
Article 21	Right to object	When the controller processes personal data for direct marketing purposes, the data party has the right to refuse to process the personal data involved in marketing purposes at any time.

In addition to the inability to identify the information of the person concerned, the principle of minimum data collection in point c of Item 1 of Article 5 (Personal Data Processing Principles of the Regulations) shall also be observed, which means that the personal data shall be appropriate, relevant, and limited to the minimization of necessary data related to processing purposes.

Article 8 of the regulation refers to the conditions for children's consent in information society services, which are divided into three items. Item 1: if a child is 16 years old or older, it is legal to process the child's personal information, but if the child is not 16 years old, such processing must be authorized by the consent of the legal guardian. However, EU Member States can define a lower age for passing the law, provided that the minimum age is not less than 13 years old. Item 2: under the available technology, the controller shall make reasonable efforts to verify whether the legal representative agrees or authorizes. Item 3: (1) shall not affect the general regulations of EU Member States, such as the provisions on the validity, formation, or impact of regulations related to children.

Article 17, right to erasure, is also called right to be forgotten, and its provisions are divided into three items. Item 1: when personal information is no longer needed or is illegally processed, data parties shall have the right to obtain the deletion of personal information from the controller without unreasonable delay, and the controller has the

obligation to delete personal information. Item 2: if the controller discloses personal information, according to Item 1 of this article, and if the data party requires deletion, the controller shall delete any connection or copy related to the data. Items 1 and 2 of these articles do not apply when Item 3 is to exercise the right to freedom of expression and information or to establish, exercise, or defend legal requirements.

The right to object in Article 21 of GDPR is divided into six items. The first item expressly stipulates that the data party has the right to refuse the regulations based on specific circumstances. Point e or f of the first item deals with relevant personal information, including all filing of this provision, unless the controller proves that the processing was prior to the legal basis, establishment, exercise, or defense of the rights and freedoms of the data party. Otherwise, the controller shall not process personal data. Item 2: when personal information is processed for direct marketing purposes, the data parties have the right to reject the scope of data processing involved in marketing purposes at any time.

Item 3 of the right of refusal is as follows: when the data party refuses to process for direct marketing purposes, such purpose processing will no longer occur. Item 4: when communicating with the data parties for the first time, the rights of Items 1 and 2 shall be clearly put forward, and the difference between any information shall be clearly introduced. Paragraph five states that in the process of using information society services, despite the provisions of Directive 2002/58/EC, data parties may refuse to use the automated methods of technical specifications. Paragraph six states that if the processing of personal data is for scientific, historical, or statistical research purposes in accordance with paragraph one of Article 89, the data party shall have the right to refuse the processing of relevant personal information.

In this paper, the server side of Figure 2 is detailed in Figure 3. The system combines the five GDPR clauses in Table 2 with the server-side user interface functions, as shown in Figure 3. On the server side, there are three kinds of running functions: sending and receiving instructions, fetching status, and user interface. The socket server is used for sending and receiving instructions. The user control end transmits the sent instructions to the socket server. At this time, the socket server transmits the received instructions to the device control end and transmits the device control status to the database for recording. The crawl status function displays the information in the database through the web page.

The user interface function provides six functions, including adding users, adding devices, logging off devices, deleting records, viewing device status, and viewing history. When adding users and new devices, the system writes the new results to the database. Logging off the device and deleting the record removes the corresponding data in the database. Viewing the device status and viewing the history displays the data in the database. Among them, new users, new devices, cancelled devices, and deleted records are combined with GDPR provisions into the function.

When new users are added, the family may include minors, so the age judgment function was added to protect minor children. This design needs to ask whether users are 13 years old or older, and if they are at least 13 years old, it must ask whether they are 16 years old or older. This step is to comply with the conditions for the consent of children involved in information society services. After completion, new users can be added.

The newly added equipment functions should comply with the principle of pseudonymization, minimum data collection, and the right of refusal. Kana is used to record the name of the device, which is customized by the user. In terms of data collection, this paper refers to [41] to summarize the personal information most frequently collected by suppliers, and the data collected by this system are described in Table 3. As shown in Table 3, the system follows the principle of minimum data collection, as it collects equipment status information but excludes equipment values. The right of refusal is provided to the user to refuse to collect data, and the user can decide whether to accept the data collected by the system according to his own investigation.

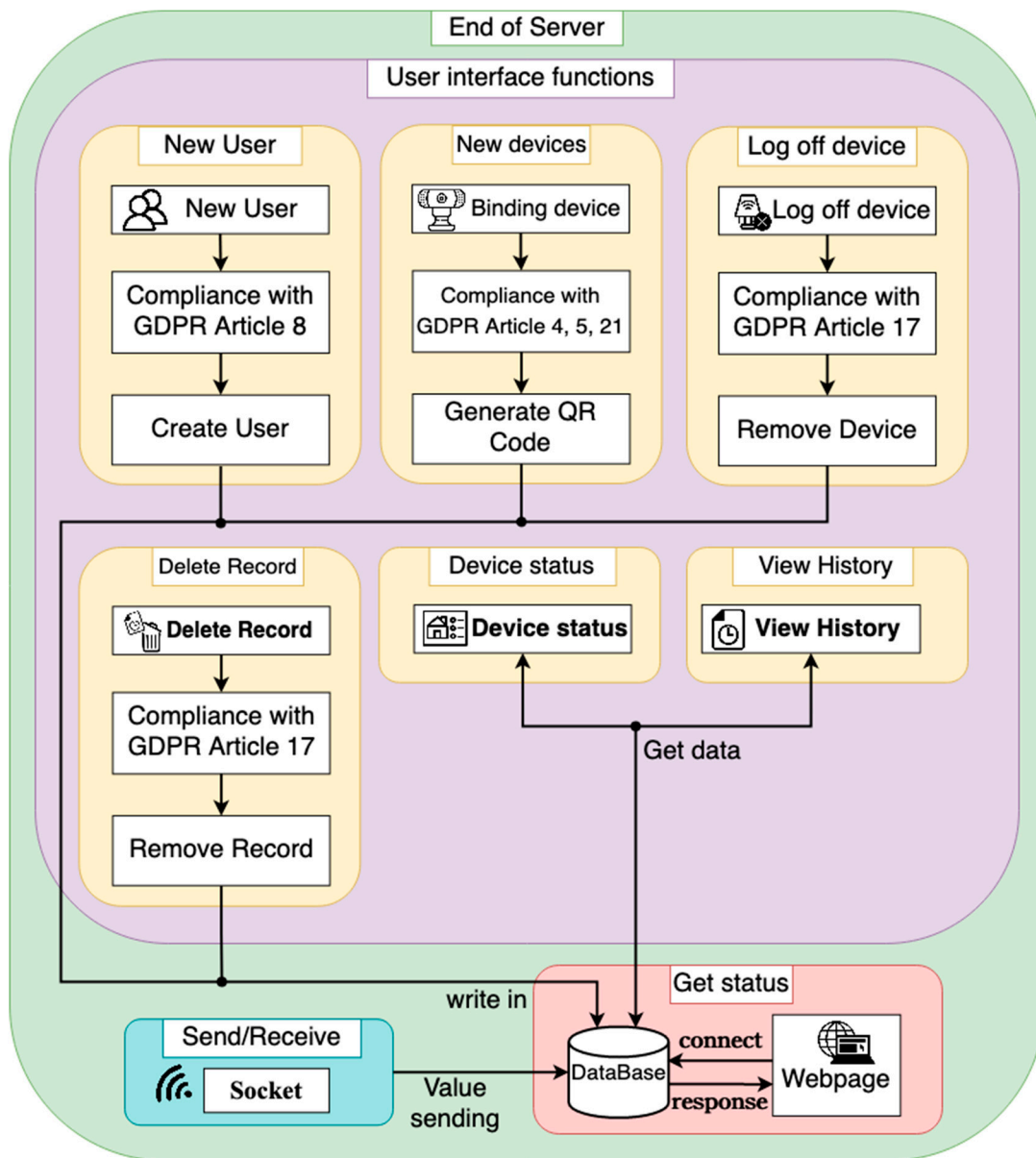


Figure 3. Schematic diagram of server module.

Table 3. Data collection.

	Item	Collect	Do Not Collect
1.	Equipment use status	✓	
2.	Equipment service time	✓	
3.	User email	✓	
4.	Equipment serial number	✓	
5.	Equipment name	✓	
6.	Position		✓
7.	Personal preference		✓
8.	User name		✓
9.	ID card No		✓
10.	Card number		✓

The system has the right to delete the contents of the clauses. When the user needs to remove the equipment or wants to remove the collected information, he/she can perform two functions at any time, namely, logging off the device and deleting the record. If the user executes this function, he/she cannot view the historical record or query the device information. In other words, if deleted, it will be deleted together with the data accessed at that time in the database, leaving no records.

3.2. Equipment Data Format Conversion

Data format refers to the format of data storage records or files of hardware devices. Generally, the types of formats are numerical, binary, octal, or hexadecimal. However, the data formats used by various hardware equipment manufacturers on the market are different. When users buy products from different manufacturers, they need to use the application programs developed by the manufacturers themselves, which causes inconvenience to users.

In order to provide users with multiple choices for household appliances, the system performs data format conversion for household appliances. Figure 4 shows a schematic diagram of the conversion of binary data to the hexadecimal format. Since the device formats provided by various manufacturers are different, it is necessary to connect the home appliance with ESP32 first. After ESP32 connects with the home appliance, it reads the data format of the home appliance and uniformly converts the data to the hexadecimal format through the program.

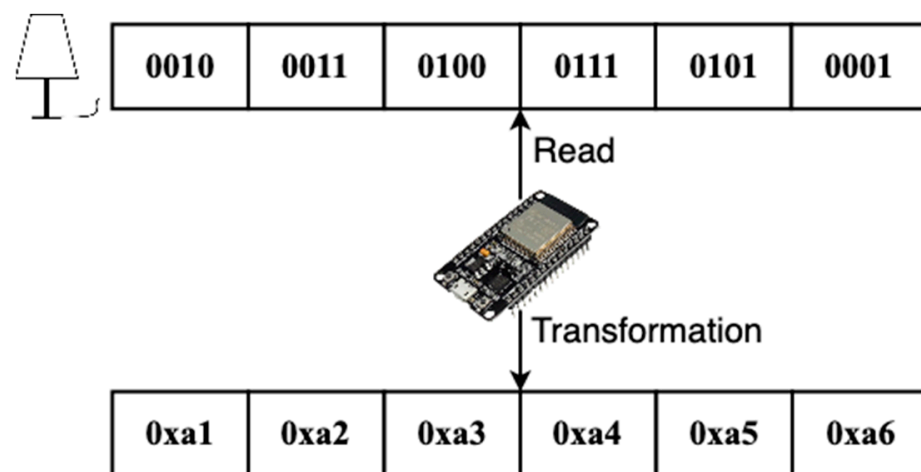


Figure 4. Schematic diagram of converting binary data to the hexadecimal format.

After the device data format is converted by ESP32, the wireless network can be used to transmit packets to the server through the socket. The server confirms the identity of the device by the header and footer of the received packets. As shown in the packet information diagram in Figure 5, the system distinguishes packets of household appliances of different brands by different headers and tails. If the header of packets received by the server is 0xa1 and the tail of packets is 0xa5 and 0xa6, the household appliances can be determined to be A-brand LED.

Except for the header and footer, the rest of the packet is the device information. When the status of the appliance changes, the device control terminal writes the information into the packet, and the server knows the appliance status through the middle section of the packet. The user control end uses the same principle to write the instruction to be controlled into the packet and transmits the packet to the device control end through the socket server. The device control end will change the status according to the received packet.

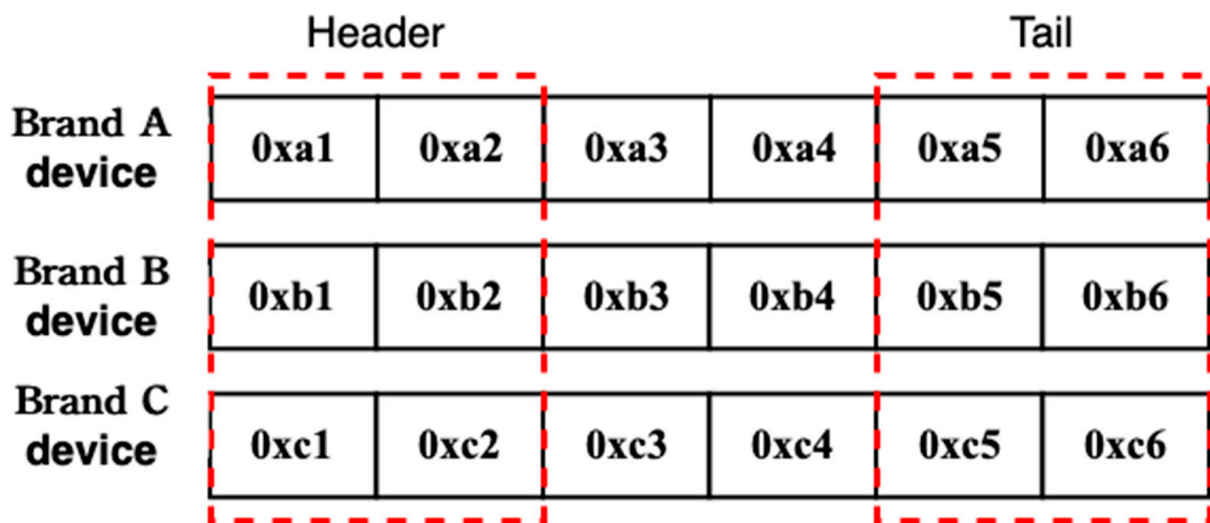


Figure 5. Schematic diagram of packet information.

3.3. Consensus Mechanism

In modern life, the IoT is widely used and convenient. However, with the increasing number of IoT devices, determining how to ensure data security is a major challenge for developers. The security risk of the IoT not only relates to data theft but also to the use various methods to maliciously attack or control appliances. If developers ignore IoT security issues, it may bring inconvenience or danger to users' lives.

For IoT security issues, the system adds consensus mechanism technology to improve security and to quickly ensure that devices are controlled by people with a mind. At present, there are many kinds of consensus mechanisms, each of which has its own advantages, disadvantages, and different functions. The system uses the concept of the Byzantine general problem to reach a consensus between each device control end and the user control end. If one node does not match the information of other nodes, it can be determined that the device is controlled by someone with a mind.

The schematic diagram of the consensus mechanism module of the system is shown in Figure 6. When the user control terminal operates device control terminal two, the user control terminal transmits a log file to device control terminal one, device control terminal two, and device control terminal three, and the operated device control terminal two also transmits the log file to device control terminal one, device control terminal three, and the user control terminal for confirmation. The contents of the log file are the MAC address, the changed state of the equipment, and the time of the changed state of the equipment. If a hacker invaded device control terminal one and operates it, device control terminal one would transmit the log file to device control terminal two, device control terminal three, and the user control terminal, while other terminals would not send out the log file. At this time, it can be known that the operation of device control terminal one is not performed by a family member.

Algorithm 1 shows that the user control terminal operates the virtual code of device control terminal two. The user control terminal writes the MAC address of the device to be controlled, the status to be changed, and the execution time to the log file and sends the log file to all device control terminals. The device control end being operated writes the MAC address, changed status, and execution time to the log file and sends them to the other device control ends and user control ends.

Algorithm 1 Pseudocode of user control terminal operating device control terminal 4

```

1.  let user = User control terminal
2.  let device_1 = Equipment control terminal 1
3.  let device_2 = Equipment control terminal 2
4.  let device_3 = Equipment control terminal 3
5.  let user_log = Log file of user control terminal
6.  let device_2_log = Log file of equipment control terminal 2
7.
8.  # User-operated equipment 2
9.  User sends command to device 2
10. user_log = MAC address, status to be changed, and execution time of the device 2
11. Send user_Log to device 1, device 2, and device 3
12.
13. if device_2 Receive instructions
14. device_2 Implementation status change action
15. Device_2_log = MAC address, change status, and execution time of device 2
16. Send device_2_Log to device_1, device_3, and user
17. else
18. Do not perform actions

```

The device control terminal judges whether the operation is a family member virtual code, as shown in Algorithm 2. When device control terminal one receives the log files of the user control terminal and device control terminal two, it first judges whether the information of the log files of the user control terminal and the device control terminal are consistent. If the information of the two files is consistent, it can be determined that the operation is conducted by a family member. If the information is inconsistent, it can be determined that the user control terminal is not operated by a family member. If device control terminal one only receives the log file of device control terminal two, it can be determined that the operation of device control terminal two was performed by a hacker.

Algorithm 2 Virtual code for judging operation result at equipment control terminal

```

1.  let user = User control terminal
2.  let device_1 = Equipment control terminal 1
3.  let device_2 = Equipment control terminal 2
4.  let user_log = Log file of user control terminal
5.  let device_2_log = Log file of equipment control terminal 2
6.
7.  if device_1 Received user_Log and device_2_log
8.  # Check the log content
9.  If user_log == device_2_log
10. Decide to act as a family member
11. else
12. User is not a family member
13. else if Only device is received_2_log
14. Confirm that the device has been hacked
15. else
16. Waiting to receive

```

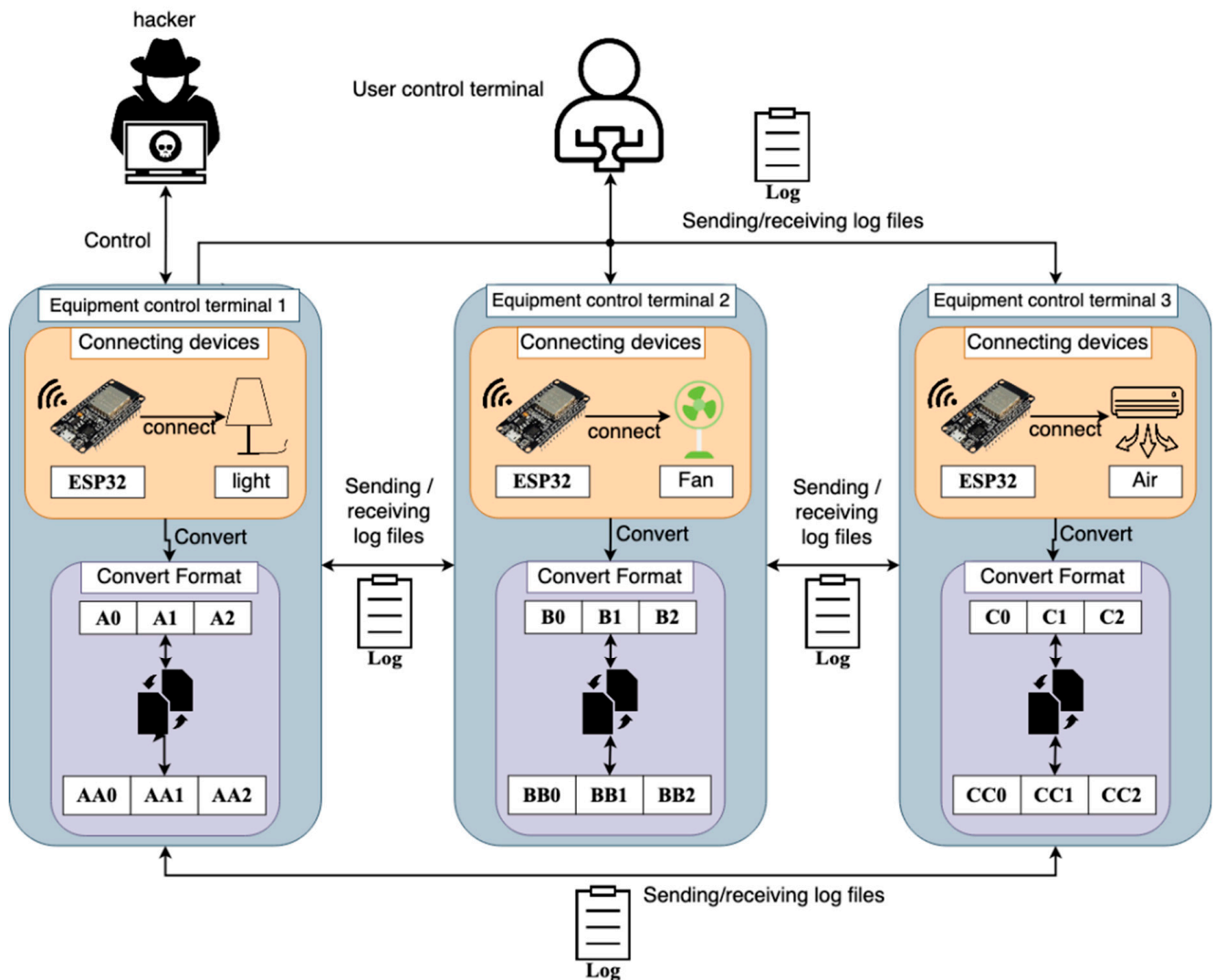


Figure 6. Schematic diagram of consensus mechanism module.

4. Research and Analysis

This paper combined GDPR with IoT technology applications and provided a user interface and user interaction in the server. Figure 7 shows the operation sequence between the user and the server. First, the user creates a new user in the server. During the process of creating the user, the server asks the user about the GDPR clause, and the user replies to the clause. After the server confirms that the user’s account format is correct and the fields are filled in, the new user is successfully created.

After the user logs in with the newly created user account, the server checks whether the account exists in the database and then confirms whether the password is correct. If both are correct, the system will jump to the interface for entering the verification code. Then the server randomly generates a group of verification codes. The server writes the verification codes into an email and sends a letter to the user’s mailbox. The user needs to enter the verification code in the letter into the field. After the server compares the correctness of the verification code entered by the user, the interface jumps to the control interface.

The user operation’s initial screen is shown in Figure 8. This is the user operation interface, which provides three functions: user login, account application, and password forgetting. To improve security, the system limits the user account format to the email format, uses email to verify whether the user is himself or herself, and prevents the account from being stolen by intentional persons. The system will hide the password in the password input field, providing an environment for users to enter the password safely.

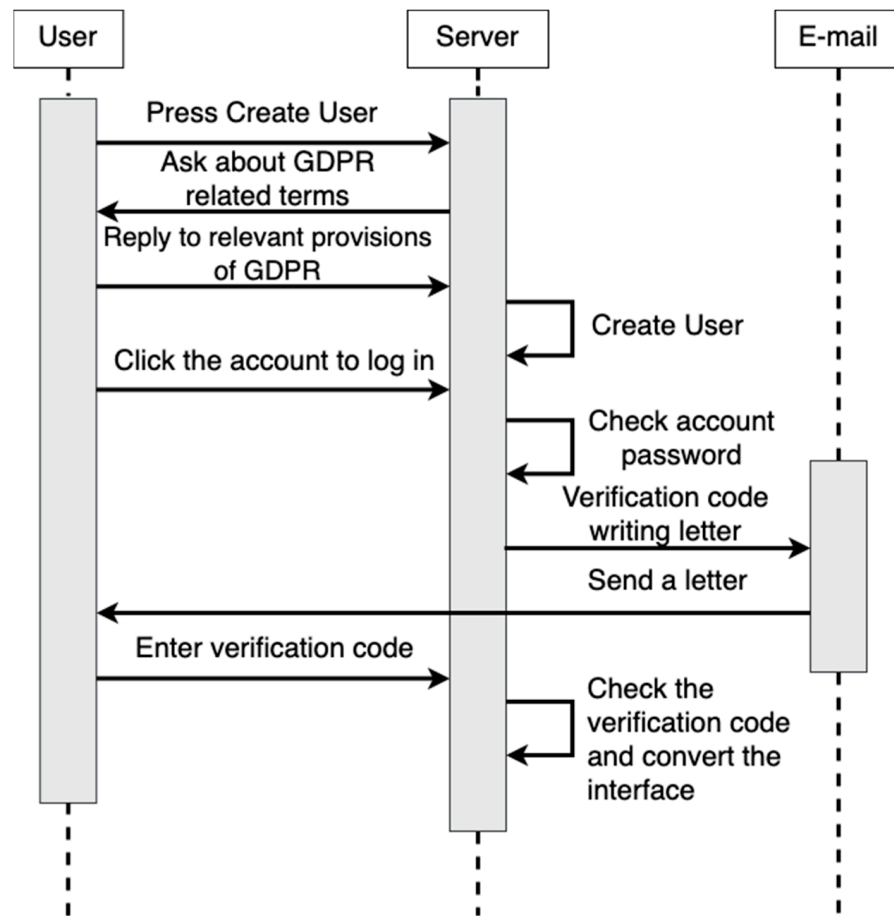


Figure 7. Sequence diagram of user and server operation.

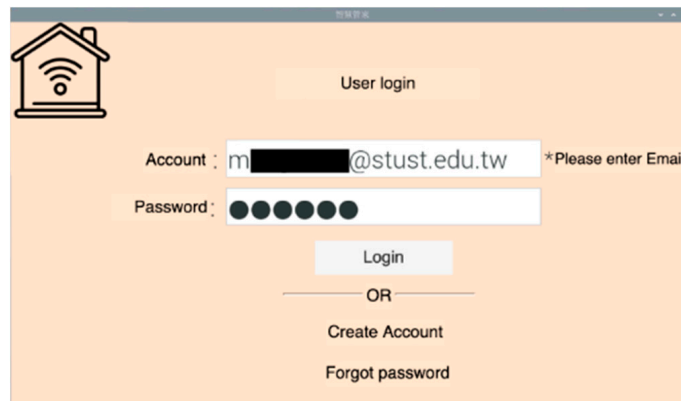
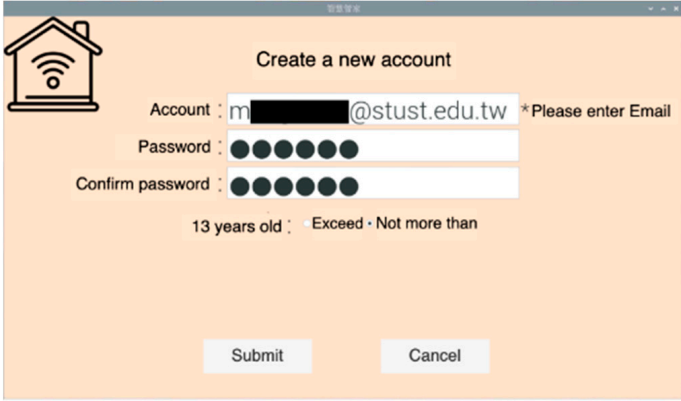


Figure 8. User operation interface.

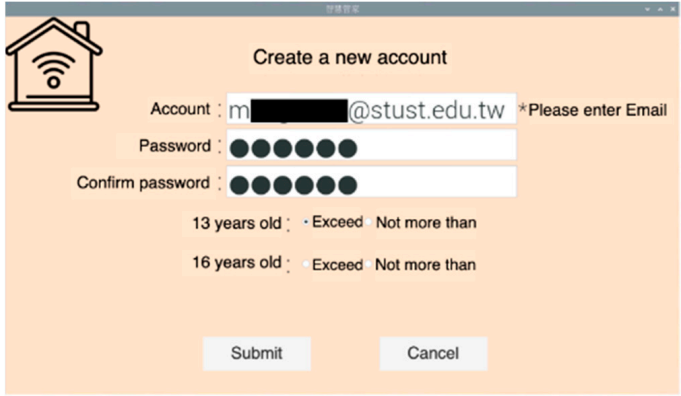
The account application function abides by Article 8 of GDPR: comply with the consent conditions that involve information society services for children. In Article 8, it is necessary to first pay attention to whether the user’s age is 13 years old, as shown in Figures 9 and 10, because it is stipulated that the minimum age is 13 years old. As shown in Figure 9, when the user clicks the option under 13 years old, the system will send it directly without asking for more details and will unconditionally not collect any relevant information from the user in accordance with the provisions. As shown in Figure 10, if the user clicks the option of 13 years old or older, the system will pop up the option of asking whether the user is 16 years old or older.



The screenshot shows a web browser window titled "Create a new account". On the left is a house icon with a Wi-Fi signal. The form contains the following fields and options:

- Account : m [redacted] @stust.edu.tw *Please enter Email
- Password : [redacted]
- Confirm password : [redacted]
- 13 years old : Exceed Not more than
- Submit and Cancel buttons.

Figure 9. Interface of account creation under 13 years old.

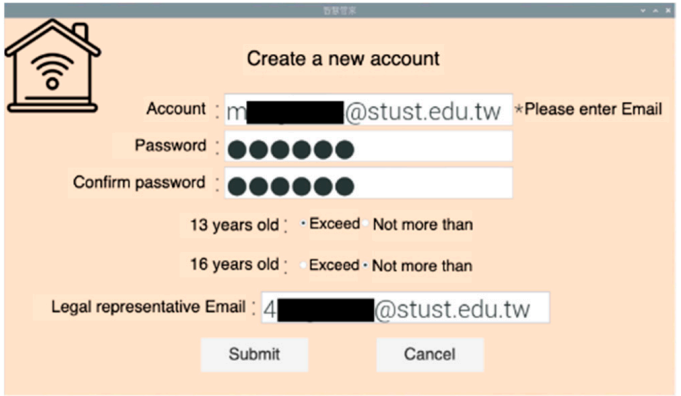


The screenshot shows the same "Create a new account" interface. The form contains the following fields and options:

- Account : m [redacted] @stust.edu.tw *Please enter Email
- Password : [redacted]
- Confirm password : [redacted]
- 13 years old : Exceed Not more than
- 16 years old : Exceed Not more than
- Submit and Cancel buttons.

Figure 10. Interface of account creation age over 13.

According to Item 1 of Article 8 of the GDPR, it is legal to process the personal information of users who have reached the age of 16. If the service provider needs to collect the personal information of users who have not reached the age of 16, it is legal only when authorized or agreed to by the legal representative. As shown in Figure 11, when the user indicates that he/she is under the age of 16, the system will pop up and fill in the legal representative email field to be authorized by the legal representative. To comply with the provisions of Item 1, Article 8 of the GDPR, the user must fill in the legal representative email before creating. As shown in Figure 12, if the user clicks the option of over 16 years old, the user can decide the use of personal information by himself/herself without the authorization of the legal representative.



The screenshot shows the "Create a new account" interface with an additional field for legal representative email. The form contains the following fields and options:

- Account : m [redacted] @stust.edu.tw *Please enter Email
- Password : [redacted]
- Confirm password : [redacted]
- 13 years old : Exceed Not more than
- 16 years old : Exceed Not more than
- Legal representative Email : 4 [redacted] @stust.edu.tw
- Submit and Cancel buttons.

Figure 11. Interface of account creation under the age of 16.

The screenshot shows a web browser window with a light orange background. In the top left corner, there is a house icon with a Wi-Fi signal. The title of the page is "Create a new account". Below the title, there are three input fields: "Account" with the text "m[redacted]@stust.edu.tw" and a note "*Please enter Email"; "Password" with six black dots; and "Confirm password" with six black dots. Below these fields, there are two lines of text: "13 years old : · Exceed · Not more than" and "16 years old : · Exceed · Not more than". At the bottom of the form, there are two buttons: "Submit" and "Cancel".

Figure 12. The interface of account establishment when the age is over 16.

After being inquired by the system, the user can create a new user account and log into the user operation interface from this account. The user needs to input the applied account password into the field, and the system will confirm whether the account exists and whether the password is correct in sequence. After confirmation, the system jumps to the screen of entering the verification code and generate a group of verification codes. This verification code is sent to the user's letter by email. The user needs to fill the verification code in the letter into the field. After the system confirms that the verification code is correct, it can jump to the user control interface.

If the user enters the verification code input interface but has not received the letter for a long time, the user can click the re-send verification code function, and the system will re-generate a set of verification codes and send them to the user's email. This system uses the verification code mechanism to send by email. To ensure that the user is himself, even if someone embezzles the account, the user can find out from the verification code letter and change the password.

Then this paper introduces the user operation interface, which provides five main functions and convenient viewing time for users. Four GDPR clauses are combined in the functions of adding devices, canceling devices, and deleting records. Users can decide the access and use of personal information under the protection of the clauses.

The new device functions need to be matched with the webcam. In order to unify the format of household appliances, the system needs to obtain the information of the original household appliances first. First, the user can scan the QR code of the original home appliance. Then the system will capture the required part of the scanned information, such as the manufacturer's license, device name, and device serial number, and then display the captured QR code information in the device information interface of the new device.

This system combines Article 4 (pseudonymization), Article 5 (principle of minimum data collection), and Article 21 (right of refusal) of GDPR. In combination with Article 4, the system provides users with the ability to name household appliances according to their own preferences so as to prevent data information from being unrecognizable when it is stolen. As the system only obtains the manufacturer's brand, equipment name, and equipment serial number (but not other information), it complies with Article 5. The user is asked whether to record the historical status. If the user does not want to record, the provisions of Article 21 can be implemented. After the user fills in the information, the system will generate a new QR code, which will be used to bind the device at the user control end.

The deletion right in Article 17 of GDPR is combined in the function of canceling the device and deleting the device. When the user can delete the device or the use record of the device he wants to cancel, he can implement Article 17 to cancel or delete the device at any time. When indicating the device to be logged off or the record to be deleted, the system will pop up the option of reconfirmation. In order to prevent the user from accidentally

clicking, the user needs to enter a password to ensure that the user can only log off or delete the record if it was not accidentally clicked.

This function of viewing device status interface is used to provide users with information about the device. In this paper, LED (LED small bulb) and FAN (motor fan) were used as experimental equipment. The nickname refers to the name that the user chooses for the device. The serial number is the original serial number of the appliance. Whether or not to record the status selected by the user is whether or not to record the status. If the user selects no, the device status cannot be known in this interface. The status is the current use status of the device.

Users can query the status and time of equipment changes through the view history function. In this paper, LED (LED small bulb) and FAN (motor fan) were used as experimental equipment. LED has two states, namely, on and off. The FAN has four states, namely, close, small, middle, and big. In addition to the user operation interface on the server side, the system also provides the user control side and the web page version to view the history. Users can use computers or mobile phones to query the history of the device at home without going to the device to operate.

The user control end of this system is a self-developed mobile application using Flutter as the framework and Dart as the program language. Figure 13 shows the user control terminal login sequence. When the user enters the account and password at the device control terminal to log in, the device control terminal confirms to the server whether there is such an account. After confirming that the account exists, the server confirms whether there was an error in entering the password. After confirmation, the server returns the result to the user control terminal.

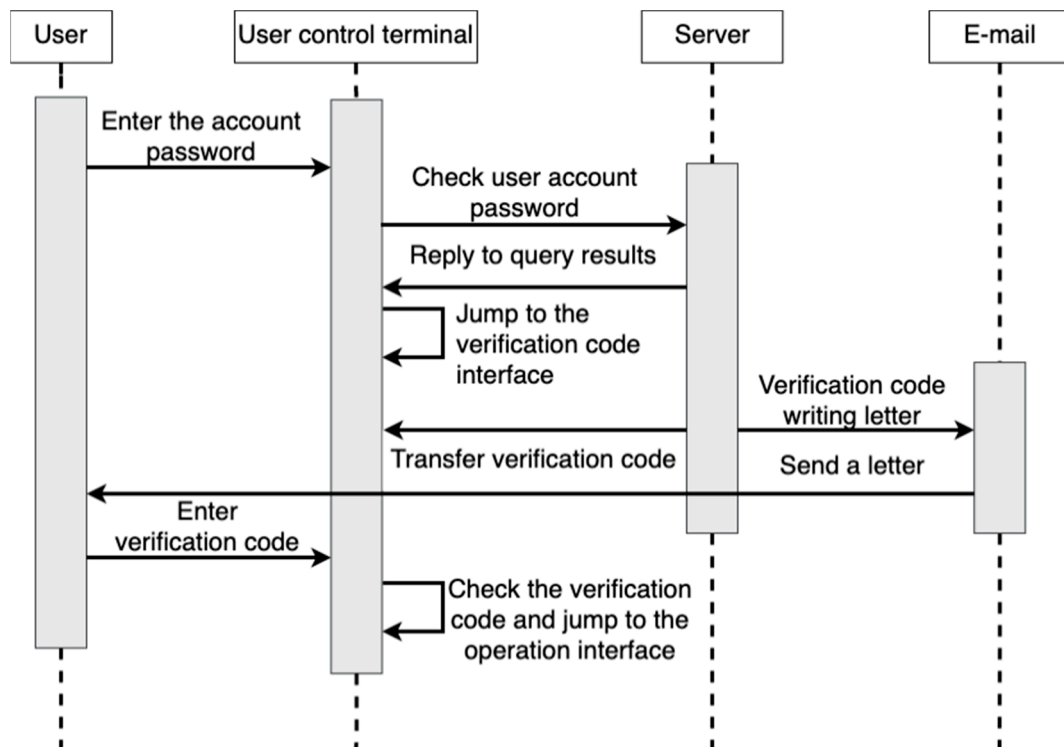


Figure 13. Sequence diagram of user control terminal login.

Currently, the user control terminal performs interface conversion, and the server generates a group of verification codes and sends them back to the user control terminal. At the same time, the verification codes are sent to the user email. The user needs to input the verification code in the email into the verification code interface. After the verification code is identified as correct through comparison, the user control terminal will convert the interface.

A sequential diagram of the user's operation on the device control terminal is shown in Figure 14. After the user presses the device start button (device control terminal one), the user control terminal first sends the command to the server, and the server sends the device start command to device control terminal one after receiving the command. After receiving the command, device control terminal one starts the device and transmits the log file of device control terminal one to the user control terminal and device control terminal two. The log file of the user control terminal is also transmitted to device control terminal one and device control terminal two. Currently, device control terminal two needs to confirm the log files of the user control terminal and device control terminal one.

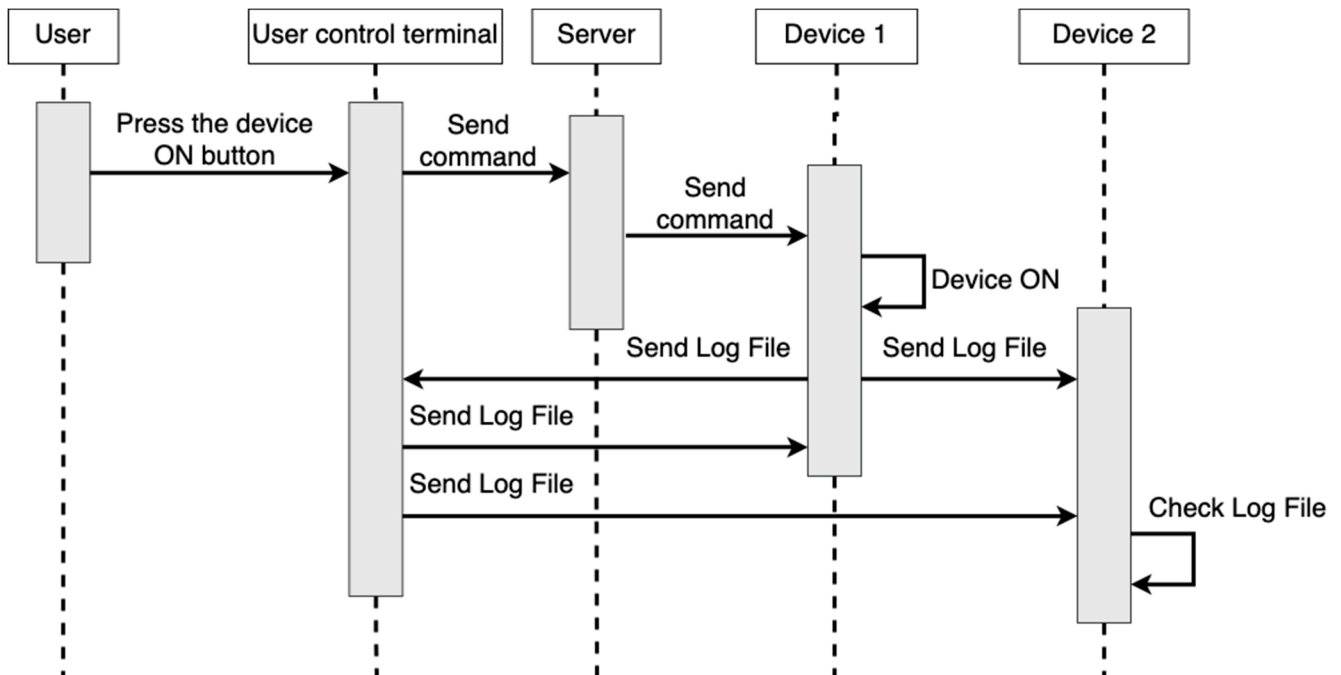


Figure 14. Sequence diagram of user control equipment.

In addition, we collected questionnaires from 70 people, including 34 people aged 16–30 and 36 people aged 31–65. A total of 67 people wanted to buy smart home appliances, 52 people wanted to buy smart home appliances of different brands, and 59 people believed that if different brands are not compatible, it would indeed affect their willingness to use smart home appliances. However, nearly 32 people could not accept smart home appliances to record personal information. However, if the GDPR specification was put on smart home appliances, about 90% of people could accept smart home appliances. If smart home appliances could be compatible with a unified format with different brands, about 97% of people could accept smart home appliances. Therefore, we recommend smart system products. If they are popular with the public, we suggest that the GDPR specification and the transmission formats of different brands can be unified and introduced into smart system products, which will make more people willing to accept them.

5. Conclusions

This paper adds GDPR data protection specification to IoT intelligent housekeeper equipment in order to achieve GDPR data protection specification. Compared with cases where the GDPR system is not used, this system, based on complying with the principle of minimum collection of GDPR data, keeps the user's personal data confidential and protected by means of pseudonymization of GDPR, making it impossible for interested persons to identify the data subject when stealing data. In addition, the user can decide whether the data needs to be recorded according to personal inspection through the GDPR

refusal right. Compared with the existing system, the user has more choices in terms of recording personal data.

Compared with the existing service communication architecture and standards in the smart home industry, the main advantage of this research was to propose a unified device data format protocol. Each product can communicate with each other through a smart housekeeper and can keep the personal information collection between its own product and users based on the personal data protection law. Therefore, the protection of personal information is relatively complete. In addition, we also proposed a consensus mechanism to ensure the security of the user's equipment. Through the Byzantine general problem method, we can determine whether the equipment is controlled by the owner. In this study, the concept of consensus mechanisms was used as the protection judgment standard for equipment safety. Through the consensus mechanism, each device end generates an independent log file. When a malicious person intrudes, the user receives the log data of the intrusion device, but it does not send the relevant operation log information. In this way, users can know the important information about the intrusion of the device so that they can take corresponding measures at the first time.

This paper contributes to the research literature in four major areas: (1) using the unified device data format protocol, each product can converge and transmit information to each other, and each product can maintain data collection with users; (2) designed and imported GDPR data protection mechanisms into the smart home appliance IoT platform; (3) increased the lifetime, interaction, and thoroughness of interest groups; and (4) promoted people's willingness to use the smart family system to realize these goals.

Author Contributions: Conceptualization, G.-J.H.; methodology, Y.-H.Y. and Y.-Y.J.; software, Y.-H.Y.; validation, Y.-H.Y., G.-J.H. and Y.-Y.J.; investigation, Y.-H.Y.; resources, G.-J.H.; writing—original draft preparation, Y.-H.Y. and Y.-Y.J.; writing—review and editing, G.-J.H. and Y.-Y.J.; supervision, G.-J.H.; project administration, G.-J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported in part by the National Science and Technology Council (NSTC) of Taiwan under Grant NSTC 111-2622-E-218-005- and in part by the Allied Advanced Intelligent Biomedical Research Center, STUST from Higher Education Sprout Project.

Conflicts of Interest: The authors declare no conflict of interest. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; Aharon, D. *Unlocking the Potential of the Internet of Things*; McKinsey Global Institute: New York, NY, USA, 2015.
2. Stăncioiu, A. The fourth industrial revolution industry 4.0. *Fiabil. Şi Durabilitate* **2017**, *1*, 74–78.
3. SEMI Taiwan. *Industry 4.0, Understand It from Shallow to Deep!* Available online: <https://www.semi.org/zh/blogs/technology-trends/industry-4.0> (accessed on 31 May 2022).
4. Biswas, A.R.; Giaffreda, R. IoT and cloud convergence: Opportunities and challenges. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Republic of Korea, 6–8 March 2014; pp. 375–376. [CrossRef]
5. Taiwan Network Information Center. 2019 Taiwan Network Report. Available online: https://www.twnic.tw/doc/twrp/201912_e.pdf (accessed on 11 July 2022).
6. Top Service Group. Do you Agree to Use Cookies for Tracking? Comply with the EU GDPR Cookie Policy. Available online: <https://www.tsg.com.tw/blog-detail3-200-0-gdpr-2.htm> (accessed on 10 July 2022).
7. Weber, R.H. Internet of things—Need for a new legal environment? *Comput. Law Secur. Rev.* **2009**, *25*, 522–527. [CrossRef]
8. Mainetti, L.; Mighali, V.; Patrono, L. A location-aware architecture for heterogeneous building automation systems. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 1065–1070. [CrossRef]
9. OOSGA. IoT Internet of Things—Definition, Application Fields and Actual Industrial Cases. Available online: <https://zh.oosga.com/iot/> (accessed on 15 December 2020).

10. The "Only" Coke Machine on the Internet. Available online: https://www.cs.cmu.edu/~{}coke/history_long.txt (accessed on 5 June 2022).
11. Shrouds of Time: The History of RFID. Available online: <https://www.railwayresource.com/company/732913/whitepapers/2291/shrouds-of-time-the-history-of-rfid> (accessed on 5 June 2022).
12. Ashton, K. That 'Internet of Things' Thing. Available online: <https://www.rfidjournal.com/that-internet-of-things-thing> (accessed on 5 June 2022).
13. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2014**, *17*, 243–259. [CrossRef]
14. Al-Qaseemi, S.A.; Almulhim, H.A.; Almulhim, M.F.; Chaudhry, S.R. IoT architecture challenges and issues: Lack of standardization. In Proceedings of the 2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 6–7 December 2016; pp. 731–738. [CrossRef]
15. Tan, L.; Wang, N. Future internet: The Internet of Things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010; pp. V5-376–V5-380. [CrossRef]
16. Internet of Things, Wikipedia. Available online: https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1096416377 (accessed on 5 July 2022).
17. Jamali, M.A.J.; Bahrami, B.; Heidari, A.; Allahverdizadeh, P.; Norouzi, F. (Eds.) IoT Architecture. In *Towards the Internet of Things: Architectures, Security, and Applications*; Springer International Publishing: Cham, Switzerland, 2020; pp. 9–31. [CrossRef]
18. GDPR. A User-Friendly Guide to General Data Protection Regulation (GDPR). Available online: <https://www.gdpreu.org/> (accessed on 5 June 2022).
19. EUR-Lex. EUR-Lex—32016R0679—EN. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679,Mar.30,2021> (accessed on 5 June 2022).
20. Blackmer, W.S. GDPR: Getting Ready for the New EU General Data Protection Regulation. *InfoLawGroup LLP* **2016**, *22*, 2016.
21. General Data Protection Regulation, Wikipedia. Available online: https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=1089437849 (accessed on 6 June 2022).
22. Wilhelm, E.O. A Brief History of the General Data Protection Regulation (1981–2016). Available online: <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/> (accessed on 6 June 2022).
23. Council of the EU. Data Protection Reform: Council Adopts Position at First Reading. Available online: <https://www.consilium.europa.eu/en/press/press-releases/2016/04/08/data-protection-reform-first-reading/> (accessed on 6 June 2022).
24. Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)—First Reading, Adoption of the Council's Position at First Reading. Available online: <https://reurl.cc/ZApkLW> (accessed on 6 June 2022).
25. EUR-Lex—32016L0680—EN. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL> (accessed on 6 June 2022).
26. Li, L.; Chen, C. Differences and Reconciliation between GDPR and Taiwan's Individual Capital Laws. Available online: <https://view.ctee.com.tw/tax/10989.html> (accessed on 1 July 2022).
27. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 6 June 2022).
28. Dwork, C.; Lynch, N.; Stockmeyer, L. Consensus in the presence of partial synchrony. *J. ACM* **1988**, *35*, 288–323. [CrossRef]
29. Lamport, L. Paxos Made Simple. *ACM Sigact News* **2001**, *32*, 18–25.
30. Dwork, C.; Naor, M. Pricing via Processing or Combatting Junk Mail. In *Advances in Cryptology—CRYPTO'92*; Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, Germany, 1993; Volume 740, pp. 139–147. [CrossRef]
31. Bentov, I.; Pass, R.; Shi, E. Snow White: Provably Secure Proofs of Stake. Available online: <https://ia.cr/2016/919> (accessed on 5 June 2022).
32. Saad, S.M.S.; Radzi, R.Z.R.M. Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS). *Int. J. Innov. Comput.* **2020**, *10*, 27–32. [CrossRef]
33. Dziembowski, S.; Faust, S.; Kolmogorov, V.; Pietrzak, K. Proofs of Space. In *Advances in Cryptology—CRYPTO 2015*; Springer-Verlag: Berlin, Germany; Heidelberg, Germany, 2015; pp. 585–605. [CrossRef]
34. Howard, H.; Mortier, R. Paxos vs Raft have we reached consensus on distributed consensus? In Proceedings of the 7th Workshop on Principles and Practice of Consistency for Distributed Data, Heraklion, Greece, 27 April 2020; pp. 1–9. [CrossRef]
35. Castro, M.; Liskov, B. Practical Byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 1999), New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.
36. Mathieu, B.; Ching, A.; Chursin, A.; Danezis, G.; Garillot, F.; Li, Z.; Malkhi, D.; Naor, O.; Perelman, D.; Sonnino, A. State Machine Replication in the Libra Blockchain. Available online: <https://developers.diem.com/papers/diem-move-a-language-with-programmable-resources/2019-06-18.pdf> (accessed on 6 June 2022).
37. Pan, J.; Song, Z.; Hao, W. Development in Consensus Protocols: From PoW to PoS to DPoS. In Proceedings of the 2021 2nd International Conference on Computer Communication and Network Security (CCNS), Xining, China, 30 July–1 August 2021; pp. 59–64. [CrossRef]

38. Alfandi, O.; Otoum, S.; Jararweh, Y. Blockchain Solution for IoT-based Critical Infrastructures: Byzantine Fault Tolerance. In Proceedings of the NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 20–24 April 2020; pp. 1–4. [[CrossRef](#)]
39. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. [[CrossRef](#)]
40. Official Legal Text. General Data Protection Regulation (GDPR). Available online: <https://gdpr-info.eu/> (accessed on 13 June 2022).
41. Zaeem, R.N.; Barber, K.S. A study of web privacy policies across industries. *J. Inf. Priv. Secur.* **2017**, *13*, 169–185. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.