Homomorphic Encryption-based Solution for Data Security in Smart Furniture

Huanyu Liu *

Business School, Xianda College of Economics and Humanities, Shanghai, 202150, China

* Corresponding author email: 22141307@student.sdsisu.edu.cn

Abstract. Smart furniture is gradually entering people's lives. The special nature of smart furniture determines that it will be exposed to a large amount of private information, but the data processing behind smart furniture still lacks sufficient security. Therefore, the research topic of this paper is the possibility of using homomorphic encryption in smart furniture, and the research topic of this paper is a smart furniture data security solution based on homomorphic encryption. The research methodology of this paper is as follows: investigating the solutions and problems of mainstream smart furniture manufacturers in terms of data security and the possibility of enhancing protection with homomorphic encryption, as well as the impact on cost issues and applicability. The study shows that the use of homomorphic encryption improves the security of remote control and data transmission of smart furniture using cloud-based technologies. In addition, it increases the versatility and reduces the cost of smart furniture and improves the compatibility between smart furniture.

Keywords: Smart Furniture; Data Security; Homomorphic Encryption.

1. Introduction

In the previous research results, I can conclude the possibility of applying homomorphic encryption in smart furniture, which is a market with a broad future. Therefore, I decided to explore in depth the difference in privacy protection and cost of using homomorphic encryption in smart furniture, in order to explore whether homomorphic encryption has practical value in smart furniture.

2. The Use of Homomorphic Encryption in Smart Furniture

2.1 Applying Homomorphic Encryption Can Improve Data Security

2.1.1 Improve Security from the Software Level

In the previous research results, I can conclude that homomorphic encryption from the software level, homomorphic encryption can not only ensure the security of data transmission, homomorphic secrecy can also improve the security of data in the process of processing, there are relevant studies show that homomorphic encryption multiple attacks including but not limited to resistance to SQL attacks [1], etc. The security of users' private data is improved from all aspects [2], and the control and coordination system of smart furniture [3] is the operating condition for multiple systems to coordinate with each other, and homomorphic encryption is the best encryption for such operation and the best solution for the growing security needs of smart furniture [4]. When data is exchanged between individual smart furniture, it can be encrypted first using homomorphic encryption, so that the original data only stays in the smart furniture where the data is collected and not passed between individual smart furniture, thus achieving the security of protecting the original private data, and at the same time, the data collected by the smart furniture can be uploaded to the cloud repository to ensure that the data is more secure and the original private information of the user is not stored In the cloud library, thus ensuring that the manufacturer's accident does not affect the user's information, from the value side, for hackers, the value of the manufacturer's server is greatly reduced, but also at another level to ensure data security.

2.1.2 Feasibility of Homomorphic Encryption at the Hardware Level

Smart furniture from the hardware level of data exchange, the essence of smart furniture is the microcontroller and its data exchange is through the Internet of Things to achieve the exchange [5], and for the exchange of data between the individual pieces of smart furniture, homomorphic encryption is the best way to protect the data, smart furniture data acquisition method is through a variety of sensors, of which wireless sensors is one of the key, through the wireless-based Sensor networks in which the protection of data can be enhanced [6], from the data acquisition sensors of the microcontroller to the data transfer between the microcontroller IoT can be applied in all aspects of homomorphic encryption to implement encryption, from the theoretical level of hardware, homomorphic encryption has a high practical value in smart furniture, using homomorphic encryption, no additional hardware support is required, and the characteristics of homomorphic encryption also determine It does not require a specific ecosystem, and the data exchange between different hardware models can be achieved by maintaining uniformity among algorithms, so homomorphic encryption has a positive effect on the promotion of smart furniture from the hardware theory.

2.2 The Impact of Homomorphic Confidentiality on the Operation of Smart Furniture

Intelligent furniture from the hardware level of data exchange, intelligent furniture data exchange is through the Internet of Things to exchange, and for each individual in the intelligent furniture, the efficiency of homomorphic encryption to ensure that even the encrypted data can be run at a very high efficiency, and the application of homomorphic encryption compared to other encryption technology, is a low-cost in exchange for a high efficiency, even if the need for Even if the data needs to be encrypted, due to the efficiency of its encryption algorithm, it can be encrypted by each individual intelligent furniture. There is no need to add additional computing encryption modules, and from the theoretical level of the algorithm, homomorphic encryption has great application space among intelligent furniture. It can be seen that homomorphic encryption has very little effect on the efficiency of smart furniture, and even the use of homomorphic encryption may improve the efficiency of smart furniture compared to smart furniture encrypted with other algorithms [7]

3. Applying Homomorphic Encryption and Cost Issues

Applying homomorphic encryption in smart furniture will not only not increase the application cost of smart furniture, but even reduce the cost of smart furniture, making it more universal, using homomorphic encryption, data can be uploaded to the cloud, reducing the hardware cost, and homomorphic encryption is to ensure both data security and not to occupy too much space in the cloud, thus reducing the cost problem of smart furniture [8], and because of the efficiency of homomorphic encryption [9], it is possible to exchange encrypted data between smart furniture at a very low cost, and the use of homomorphic encryption can also solve the problem of data exchange between smart furniture manufacturers, thus making the overall compatibility of homomorphic encryption stronger, improving user experience, and reducing the cost of users from another aspect, thus further The development of intelligent furniture can be further promoted.

4. A Basic Explanation of the Operating Principles of Smart Furniture

The working principle of smart home: through various types of sensing devices to accept various types of sensing signals and trigger control commands or through the human conscious remote control, manually trigger the corresponding transmitting class of intelligent devices to retrieve control commands, and then execute the operation. For example: temperature and humidity sensors collect indoor temperature and humidity change data, set the trigger requirements for temperature and humidity change according to demand, when the temperature or humidity reaches the preset trigger requirements, linkage to retrieve control commands; when the temperature is high, the air conditioner starts cooling, when the temperature is low, the air conditioner starts heating. When the brightness

sensor is installed, the preset light will be closed when the indoor light brightness is sufficient, and the preset light will be opened when the indoor light brightness is not enough. Command launch fragment The role of the command launch fragment is to accept all kinds of sensing signals through all kinds of sensing equipment, and trigger control commands or perhaps through the human conscious remote control, manual trigger corresponding to the launch of intelligent equipment to retrieve control commands, for example: temperature and humidity sensors to collect indoor temperature and humidity change data, according to the need to set the temperature and humidity change trigger requirements, when the temperature or humidity reaches the preset trigger requirements, the linkage When the temperature or humidity reaches the preset trigger requirement, the control command is retrieved. When the temperature is high, the air conditioner starts cooling, when the temperature is low, the air conditioner starts heating. If the device is a brightness sensor, when the indoor light brightness is sufficient, the preset lights actively closed, when the indoor light brightness is not enough, the preset lights actively open. If the security body sensor, when set up defense, monitoring someone in the activity, immediately trigger the phone alarm. When the non-defense form, the induction of people, the initiative to open the preset lights; when monitoring no one, the initiative to close the lights. The above few scenes are completed by all kinds of sensors to actively sense the trigger to complete intelligent control, of course, can also be indirectly manually triggered control commands, for example: through all kinds of intelligent remote control, intelligent panels on the wall, the family LAN does not constrain a computer to indirectly trigger the control command, if people are not indoors, but also through the telephone or INTERNET long-distance control to control all indoor equipment. Command execution fragment

For example: turn on the lights or turn off the lights, important through the intelligent panel to complete, intelligent panel received all kinds of control commands, after analyzing the decoding, drive the corresponding strong power drive circuit, the light control back to the road on or off, so that the control is complete. In addition, like electrical appliances, curtains and other equipment control is the same reason, when the digital curtain switch, after receiving the control command, immediately drive the corresponding circuit of the electric curtain motor to turn on or off, so as to do the curtain switch control. The control of infrared appliances, such as air conditioners, TV sets, DVDs, etc., is accomplished through the human body sensor installed in the ceiling. After the human body sensor receives the control signal, it immediately forwards the control signal into corresponding infrared commands, such as controlling the infrared control commands of DVD players such as on/off, play, and pause. On the completion of the security alarm effect, when the digital security module, after receiving the control command, will be converted into a corresponding voice signal to call the preset phone number alarm. About the background music control intelligence, the same, when the digital audio and video center of gravity, after receiving the control command, immediately switch the external playback source circuit, and start playing the audio source. Therefore, when triggering all kinds of complex scene command, for example: "theater" scene key trigger, then the corresponding command execution equipment fragment according to the received command decoding and together with the implementation of the control command, so that the corresponding lights, appliances, curtains, background music began to one-sided according to the preset level of task, to reach the preset scene effect.

5. A Basic Explanation of the Principle of Homomorphic Encryption

Homomorphic Encryption (HEE) has become more important with the development of the Internet and the birth of the concept of cloud computing, as well as the increasing demand for ciphertext search, electronic voting, mobile code, and multi-party computing. Homomorphic Encryption is a class of encryption methods with special natural properties, which was first proposed by Rivest et al. in 1970s. Compared with general encryption algorithms, Homomorphic Encryption can achieve not only the basic encryption operation, but also a variety of computation functions between ciphertexts, i.e., computation first and decryption later can be equivalent to decryption first and computation later.

This feature is important to protect the security of information, as homomorphic encryption technology can calculate multiple ciphertexts before decryption, so that it is not necessary to spend high computation cost to decrypt each ciphertext. It can reduce the communication cost and transfer the computation task, which can balance the computation cost of each party; using homomorphic encryption technology, the decryption party can only be informed of the final result, but cannot obtain each ciphertext message, which can improve the security of information. Because of the advantages of homomorphic encryption in terms of computational complexity, communication complexity and security, more and more research efforts have been devoted to the exploration of its theory and application. In recent years, cloud computing has received a lot of attention, and one of the problems encountered in its implementation is how to ensure the privacy of data, and homomorphic encryption can solve this technical problem to a certain extent.

The more mainstream homomorphism schemes are additive homomorphism, multiplicative homomorphism, partial full homomorphism and full homomorphism. Additive homomorphism: The family of homomorphic functions supported by this encryption scheme are all functions that can be implemented by addition only. The most widely used is paillier additive homomorphism. Multiplicative homomorphism: The family of homomorphic functions supported by this encryption scheme is all functions that can be realized by multiplication only. For example, the classical RSA encryption scheme. Partially fully homomorphic encryption, somewhat homomorphic encryption or leveled fully homomorphic encryption: The family of homomorphic functions supported by this scheme are functions that can be implemented by a finite number of additions and a finite number of multiplications. fully homomorphic: the scheme can support the homomorphic function family of all additions and multiplications can be achieved by the function. For example, BGV, BFV, CKKS. Homomorphic encryption is generally asymmetric, but of course there are also homomorphic schemes with symmetric encryption. The following description uses asymmetric encryption, i.e., the terminology description of public key systems. Symmetric encryption is a symmetric encryption where the public and private keys are equal.

6. Analysis of the Implementability of Homomorphic Encryption Applied to Smart Furniture

From the above, it can be seen that homomorphic encryption can be applied in the operation of smart furniture in which the local data processing and the transfer of information between smart furniture as well as for the uploading of data from the cloud service of smart furniture. From the aspect of local data processing, it can be considered that homomorphic encryption makes use of data acquisition of smart furniture for local encryption, due to the efficiency of homomorphic encryption, thus making it possible even for smart furniture to encrypt the acquired Due to the efficiency of homomorphic encryption, it is possible to encrypt the acquired data even for smart furniture without additional computing modules, thus realizing the first step of application, the encryption of data by the data acquisition unit. From the data transfer between smart furniture, using the characteristic of full homomorphic encryption, the data can be exchanged smoothly, so that there is no compatibility problem caused by the different encryption methods of different smart furniture between different manufacturers, which means that the information processed with homomorphic encryption can be applied to the old or new versions of machines without any pressure, even between machines of different manufacturers. This is a huge cost advantage, not only for manufacturers to reduce the cost of production compatibility or software development, but also for users of goods, which is a more humane design. From the vendor's point of view, if the encrypted data is stored in the server, the vendor will face less pressure on the security of private data and public opinion, which is also a way to reduce pressure from the other side.

7. Summary

The use of homomorphic encryption in smart furniture has practical possibilities. Homomorphic encryption not only has the effect of protecting data security, but also can reduce the cost of smart furniture and improve the compatibility of data furniture, so the use of homomorphic encryption in smart furniture has strong possibilities and practicality.

References

[1] Yang YL, Peng CK, Zhou ZH. Homomorphic encryption-based solution for preventing SQL injection attacks[J]. Information Network Security, 2014(1):4.

[2] Li Meiyun, Li Jian, Huang Chao. Trusted cloud storage platform based on homomorphic encryption[J]. Information Network Security, 2012(9):6.

[3] Zhuang Xiangkun, Pan Hua. A communication and coordination system and its working method based on intelligent furniture control by Internet of Things, CN112255974A [P]. 2021.

[4] Chen Chaojun. Analysis of smart home data security under cloud computing and big data[J]. Electronic Technology and Software Engineering, 2015(20):1.

[5] Zhou Lili, Zhang Hongmei, Du Yinfu. On the design of IoT sensing architecture for smart furniture[J]. Automation Technology and Applications, 2018, 37(4):5.

[6] Guo Qibiao. Analysis of secure data fusion based on homomorphic encryption for wireless sensor networks[J]. Network Security Technology and Applications, 2015(5):2.

[7] Chen LQ, Zhang L, Zhu Z. Smart home data privacy protection method based on full homomorphic encryption, CN105577357A [P]. 2016.

[8] Shao, Yi-Wen. Research on Homomorphic Encryption Database Backup Technology [D]. University of Chinese Academy of Sciences.

[9] Chao Xia. Homomorphic encryption technology and its application[D]. Anhui University, 2013.