Sensors and Materials, Vol. 32, No. 6 (2020) 2187–2197
MYU Tokyo

S & M 2250

Multisensor-based Verification Mechanism with Encryption and Decryption on Fault-tolerant Databases

I-Te Chen,[1,2] Yu-Hsien Chiu,[3] Han-Chun Liao,[1]
Jer-Min Tsai,[4] Wen-Hsien Ho,[1,2*] and Chen-Sen Ouyang[5**]

[1]Department of Healthcare Administration and Medical Informatics, Kaohsiung Medical University,
No. 100, Shih-Chuan 1st Road, Kaohsiung 807, Taiwan
[2]Department of Medical Research, Kaohsiung Medical University Hospital,
No. 100, Shih-Chuan 1st Road, Kaohsiung 807, Taiwan
[3]AI Biomedical Research Center, National Cheng Kung University, No. 1, University Road, Tainan 701, Taiwan
[4]Department of Information and Communication, Kun Shan University, No. 195, KunDa Road, Tainan 710, Taiwan
[5]Department of Information Engineering, I-Shou University,
No. 1, Sec. 1, Syuecheng Road, Kaohsiung 840, Taiwan

(Received April 23, 2019; accepted February 21, 2020)

Keywords: POS, cryptography, threshold authentication, partial cipher

In addition to fierce intra-industry competition, chain businesses face many external problems. One problem is that the traditional stand-alone point-of-sale (POS) system has been unable to quickly grasp the operating performance and management of each branch. Another problem is that equipment costs continue to increase with the number of stores. Therefore, the Taiwan government has included cloud computing in its initiative to promote emerging smart industries. In addition, the world is actively investing in the cloud computing industry. Owing to security concerns, however, many domestic enterprises are reluctant to adopt cloud-based services. Secure cloud service applications must be developed to maintain and expand market share. We implement a Cloud Web POS 365 Platform with a multifactor and threshold authentication. Then, we use the required and threshold parameters to generate a key for encryption/decryption. Finally, we deconstruct a ciphertext to partial ciphertext segments and store it in each partial ciphertext database. Hence, this study contains 4 security levels. First, users need the required parameters including positioning information; when the machine is not in the set range, it cannot be used. Second, users need the threshold parameters stored in a radio frequency identification card and obtain enough card information to log into the system. Those parameters above are generating the encryption/decryption key. Third, we use a symmetric encryption module to encrypt data. Fourth, we design a deconstruction/reconstruction module to store partial ciphertext segments separately. Therefore, the proposed scheme is more secure than other cloud web POS systems. Moreover, its web-based architecture enables easy implementation in any platform. As a result, the proposed scheme would be effective for increasing the operating efficiency of chain businesses.

[*]Corresponding author: e-mail: whho@kmu.edu.tw
[**]Corresponding author: ouyangcs@isu.edu.tw

https://doi.org/10.18494/SAM.2020.2834

1. Introduction

According to Market Intelligence & Consulting Institute (MIC) statistics, the cloud-based service market in Taiwan is expected to grow from US$ 11.6 million in 2014 to US$ 265.3 million in 2022. The compound average growth rate (CAGR) for this period was estimated as 17.1%. Specifically, services such as cloud security, virtual desktop applications, and word processing applications have the most potential for future growth.

Nevertheless, Taiwan companies apparently lack confidence in the security and privacy of cloud-based data management systems. The main concerns include the authentication of identity, the encryption of data, the protection of data ownership, and protection against hackers. According to MIC data, the main concern of 80.2% of Taiwan enterprises surveyed was the security of cloud services. Therefore, a "secure cloud application service" must be developed to exploit business opportunities in cloud services, to reduce information security risks, and to expand market share.

Point-of-sale (POS) is an indispensable information system for many retail service industries. Owing to the rapid development of the Internet, conventional single-POS machines or single-store area network connections cannot meet the needs of various chain business types. If a chain business uses the conventional POS architecture, new stores must purchase new POS machines; with the number of stores, the costs of building and maintaining the information system increase. Therefore, the development of cloud POS systems has accelerated.

However, most of the currently used cloud POS systems have client/server architectures. The POS application must be installed on the client side, and updated data are not uploaded to the cloud in real time. Although the sales data stored in the cloud can be protected by commercially available backup and security mechanisms, the content of the information is "plaintext", which raises concerns about the security of confidential business information stored in the cloud. Furthermore, a conventional POS system cannot support the operating headquarters of chain businesses in integrating sales data for each branch for decision analysis.

The best solution for the above problem is for each branch to store data (e.g., manufacturers, customers, products, promotions, and materials) in the cloud database. Operation headquarters can then easily access large amounts of data quickly and easily via the Internet for use in business analysis and decision making. To prevent the leakage of enterprise sales data stored in the cloud service provider equipment, a "cloud POS system" can also embed encryption and decryption algorithms, and the key control mechanism. Hence, a "cloud POS system" with a secure access and transmission system is an innovative solution that enterprises can implement immediately.

The personal health record exchange system is another example that can apply our secure access and transmission system. Personal health records are important personal data that should be protected, especially when General Data Protection Regulation (GDPR) was implemented since May 23, 2018. In Taiwan, medical institutions can share patient medical records with patient consent. As a result, we believe that medical records should have a more secure protection.

2. Materials and Methods

The essential components of the proposed scheme are an advanced encryption standard (AES),(1) a threshold cryptosystem, multifactor authentication, and distributed encryption database, which are described below.

2.1 Essential components

The AES is a block cipher developed by the US National Institute of Standards and Technology (NIST). The AES was released on FIPS PUB 197 on November 26, 2001 and became the US standard on May 26, 2002, which uses 128-, 192-, or 256-bit keys to encrypt 128-bit blocks and generates ciphertext in 10 to 14 rounds.

The threshold cryptosystem requires the cooperation of several parties to perform the decryption or signature protocol. Adi Shamir developed the essential concept of the threshold scheme: take k points to define a polynomial of degree $k - 1$.(2,3) For example, suppose a (k, n) threshold scheme will be used to share secret S over a finite field F of size P, where $0 < k \leq n < P$, $S < P$, and P is a prime number. Randomly choose $k - 1$ positive integers $a_1, \cdots, a_{k-1}$, and let $a_0 = S$. Construct the polynomial $f(x) = a_0 + a_1x_1 + a_2x_2 + \cdots + a_{k-1}x_{k-1}$. For any subset of k points of $f(x)$, use Lagrange polynomial interpolation to find the coefficients a_0 of the polynomial.

In 2018, Sajjad *et al.* proposed “Multi-factor authentication using threshold cryptography,” which ensures the authenticity of the user to the system, as well as monitors whether the user has passed the biometric system as a normal or spoofed one.(4) A US patent has already been filed for an authentication system and device that includes a physical uncloneable function and uses threshold cryptography (US9946858B2).(5) The system and device described in US9946858B2 may be configured to enable refreshable shares and a staggered refreshment of shares. Moreover, US10122715B2, US10440016B2, and US10326775B2 show that the multifactor authentication is increasingly important today.(6–8)

US patent 20180097624 A1 was abandoned in 2020;(9) however, a robust computational secret sharing scheme that provides for the efficient distribution and subsequent recovery of private data was disclosed. The private data may be encrypted using the key, resulting in a ciphertext. The ciphertext may then be broken into ciphertext fragments using an information dispersal algorithm. In Bellare and Rogaway’s scheme (2020),(9) each key shares a corresponding ciphertext; as a result, they have to maintain many keys. In our proposal, we will modify US patent 20180097624 A1 to be a partial ciphertext database.(9)

2.2 Secure POS system

Although secure POS systems are rarely discussed in the literature, a US patent search reveals a “secure point-of-sale cellular telephone docking module system” (US 20040058705 A1),(10) in which a docking module executes a secure POS system for payment by credit card, debit card, and so forth. The secure POS system also performs check validation sequences so that checks can be safely accepted for sales and service transactions. The following features are essential for a secure POS:(11)

(1) Data Protection: Regardless of whether user data are stored in RAM, on a hard drive, or in the cloud, a secure POS system protects customer data from cyber theft.
(2) Key Logger Protection: A virtualization technique prevents the keyboard filter driver from collecting information from keystrokes.
(3) Remote Takeover Protection: This prevents cyber thieves from using application-agnostic screen capture technology to take over a POS network or a user desktop.
(4) Anti-sniffing for secure socket layer/transport layer security (SSL/TLS): This identifies malicious SSL/TLS connections.
(5) Pro-Active Virus Removal: This proactively defends against viruses on host devices and sends log to enterprise administrators.
(6) Anti-Memory Scrapping: This arrests memory scrapping processes by preventing other applications from accessing the memory of containerized applications.

2.3 Encrypted data search

In a 2012 study, Cengiz and Erkay proposed a method for the efficient and secure ranked multikeyword search of encrypted cloud data.(12) The search method was based on private information retrieval (PIR), which enables multikeyword queries with a ranking capability.(12) The same year, Xu1 *et al.* proposed a method for multikeyword ranked query on encrypted data (MKQE) in the cloud.(13) Most of the search methods proposed since then have only considered single keyword queries without appropriate ranking schemes. Moreover, the proposed MKQE requires only minor changes in the dictionary structure when additional keywords are introduced. Therefore, their scheme is better than previous solutions.

The MKQE increases the security of the keyword search scheme while providing an adequate efficiency of computation and communication. Ashwini and Archana proposed a method for efficient encrypted data search as a mobile cloud service, which used a lightweight trapdoor (encrypted format keyword). The scheme optimized the data communication efficiency by reducing the trapdoor size to reduce traffic.(14)

3. Proposed Scheme

The proposed scheme was implemented in corporation F, a POS platform provider. Figure 1 shows the results of our initial analysis of user demand in corporation F. Notably, corporation F required an expanded data analytics system, which was not considered in the proposed scheme.

The "POS 365 platform" already in use by corporation F was modified to obtain a "Cloud Web POS 365 Platform", which had three main features:
(1) The "Cloud Web POS 365 Platform" encrypts corporate data from each branch of the chain and saves it in the cloud database in ciphertext format. The benefits of using the POS 365 Platform to manage and control access include true data confidentiality and instant resource sharing.
(2) The "Secure Threshold Authentication Module" stores a partial key in radio frequency identification (RFID) tags for protecting authenticating secret *S*, which is the log-in key for

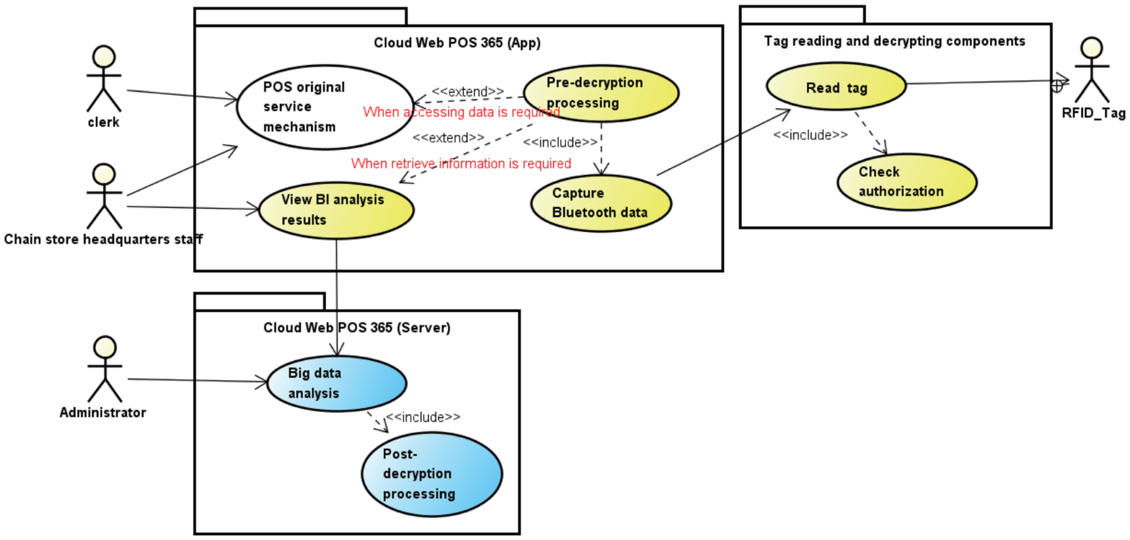

Cloud Web POS 365 (App)
clerk
Chain store headquarters staff
POS original service mechanism
<<extend>>
When accessing data is required
Pre-decryption processing
<<extend>>
<<include>>
When retrieve information is required
View BI analysis results
Capture Bluetooth data
Tag reading and decrypting components
Read tag
<<include>>
Check authorization
RFID_Tag
Cloud Web POS 365 (Server)
Administrator
Big data analysis
<<include>>
Post-decryption processing

Fig. 1. (Color online) User demand analysis chart.

the Cloud Web POS 365 Platform. The system was demonstrated using (2, 5) threshold authentication, i.e., any two of the five managers can access secret *S* and use it to log into the Cloud Web POS 365 Platform. For enhanced security, the control mechanism uses Arduino microcontrollers.

(3) After a user logs into the Cloud Web POS 365 Platform, the "Secure Encryption/Decryption and Transmission Module" accesses and transmits cloud data through an SSL/TLS channel;(15,16) the module then uses AES for data encryption or decryption.

Figure 2 shows that the three features of the platform were achieved by redesigning the Cloud Web POS 365 system architecture to include three modules:

(1) Arduino RFID tag reader and (k, n) threshold authentication module,
(2) client-side Bluetooth data capture and encryption/decryption preprocessing application module, and
(3) server-side encryption/decryption postprocessing module.

To facilitate e-commerce and e-health security, we apply cryptography, access control, radio frequency (RF) technology, and encryption/decryption, which proposes a method and system of threshold-based key verification mechanism with encryption and decryption on fault-tolerant databases. The scheme is shown in Fig. 3, which includes

(1) threshold key verification/generation mechanism,
(2) symmetric encryption/decryption mechanism, and
(3) deconstruction/reconstruction mechanism.

Through a threshold key verification/generation mechanism and the RF transmission technology, we obtain the key-related information to make a symmetric encryption/decryption key. The symmetric encryption key can encrypt a plaintext into a ciphertext and a ciphertext into a plaintext. Furthermore, the deconstruction and reconstruction mechanisms segment and reconstruct an original ciphertext, respectively. Then, the partial ciphertexts were stored in a

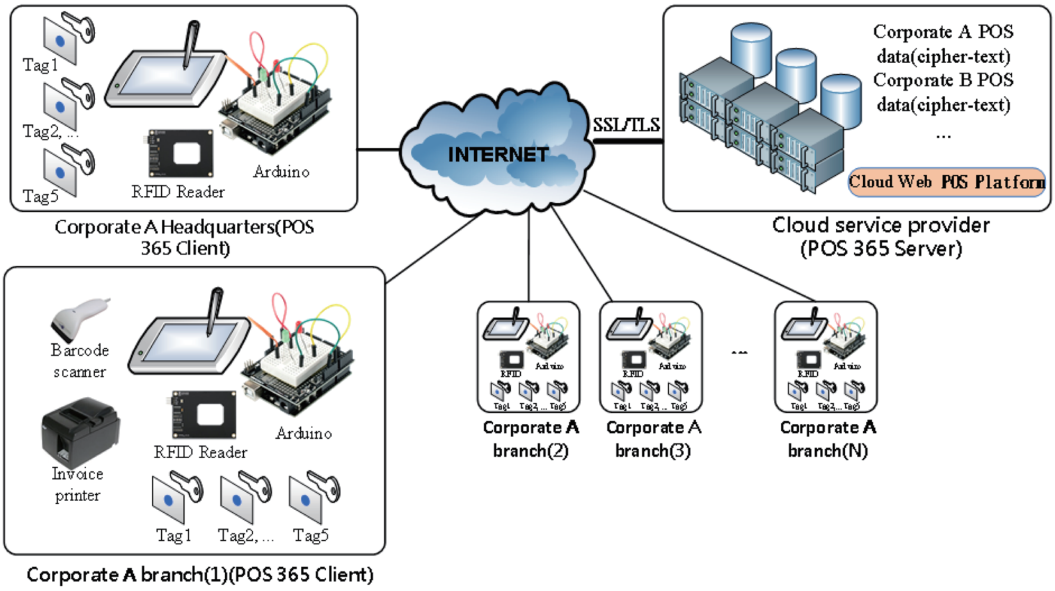


Fig. 2. (Color online) Cloud Web POS 365 system architecture.

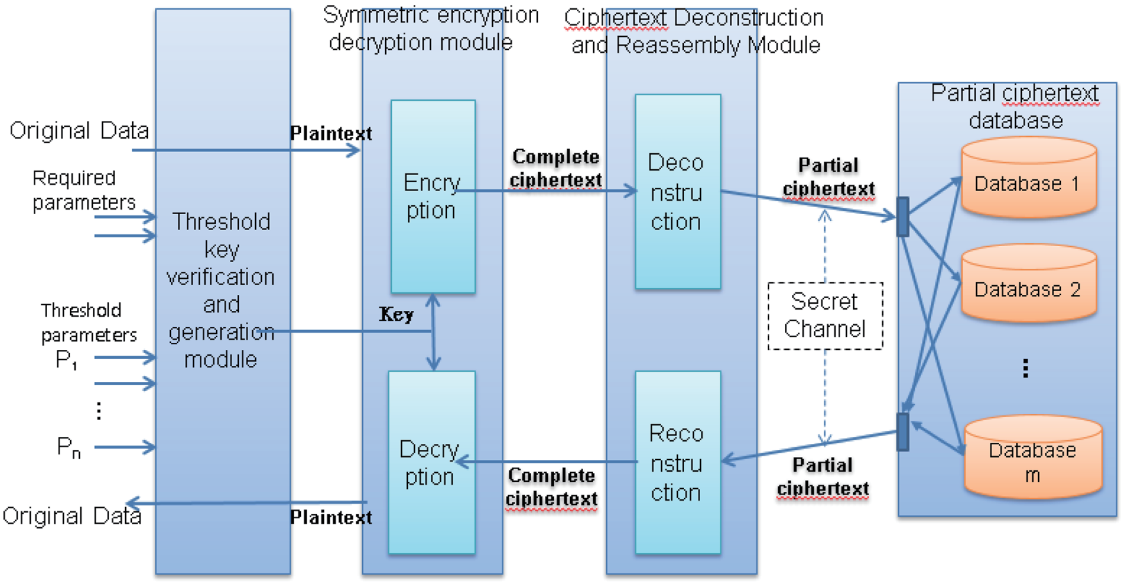


Fig. 3. (Color online) Security access transfer module activity diagram.

fault-tolerant partial ciphertext database and one can revert to the original plaintext via legal access.

In the threshold key verification/generation mechanism, the parameters include the required and threshold parameters. The required parameters can be passwords, pin codes, biometrics, latitude and longitude positioning information, and so forth. Moreover, the required parameters must be fully matched to login to the system. On the other hand, the threshold parameters are composed of one or more parameters, such as P_1, P_2, ..., P_n shown in Fig. 3; these parameters can be stored in one or more digital storage devices, such as Java Card, RFID, and NFC or an NFC-containing handheld device. When t parameters ($t < n$) are read out of n users or parameters, a seed for manufacturing the key (Seed) can be generated.(2,3) After the seed s is retrieved, we combine the seed s and the required parameters to generate random or pseudorandom numbers as the key for encryption/decryption.

In the symmetric encryption/decryption mechanism, we use the key described above and a symmetric encryption/decryption system to generate a complete ciphertext. The encryption/decryption method could be AES, 3-DES, Blowfish, IDEA, RC6, and so forth.

Finally, through the deconstruction/reconstruction mechanism, the complete ciphertext deconstructs into several partial ciphertext segments. The division method can be a Redundant Array of Independent Disks (Raid), Hamming code, Reed-Solomon codes, and so forth. Then, the partial ciphertexts are stored in more than one cloud database (such as Google Cloud, Amazon Web Service, and Microsoft Azure) through a secret channel. Moreover, we can obtain a plaintext through a reverse step mentioned above.

4. Experimental Results

Figure 4 shows the Cloud Web POS 365 Platform as an example to demonstrate our scheme.

(1) Android tablet (client side): To run Cloud Web POS 365, the client installs the AES encryption and decryption preprocessing and Bluetooth data capture components. The Local Web POS 365 App uses the Bluetooth data capture components to receive tag data from the Arduino microcontroller. If the client completes the authentication phase, the client can log into the Cloud Web POS 365 database. The Android tablet is also connected to the barcode scanner and invoice printer.

(2) RFID key control and (k, n) authentication module (Arduino MCU + RFID Reader + Bluetooth module): The Arduino MCU connects the RFID Reader and the PC, and the embedded tag memory reader and decryption component read the memory data stored in the RFID tag and transmits it to the Bluetooth data capture components.

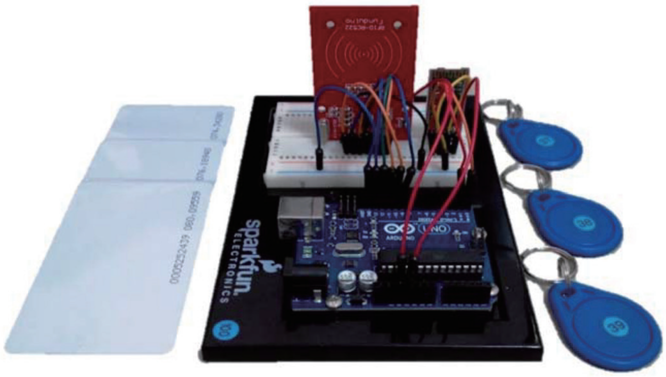


Fig. 4. (Color online) RFID key access control (Arduino + RFID Reader + Bluetooth Module).

(3) Cloud Web POS 365 Platform: The components of the Cloud Web POS 365 Platform include the program, the AES encryption and decryption processing module, the cloud database, and a large data analysis module. However, a large data analysis system is not included in the scheme described here.

After passing the (*k*, *n*) authentication module, each branch store clerk operates the original functions of the POS system as usual. When the cloud database is accessed, the encryption and decryption service mechanism can be used to view sales information in plaintext format; after new data are encrypted, they are stored in the cloud database in ciphertext format.

When the staff members of a chain store headquarters operate the original functions of the POS system, the system follows the same procedure used by the branch store clerk. The "processing" service mechanism can download and decrypt a ciphertext for sales data to view the results for various multidimensional analyses (e.g., product, gross profit, customer, performance, and store analyses).

The Cloud Web POS 365 Platform was designed for a company in Taiwan. Therefore, some texts in the following figures appear in traditional Chinese. However, English translation is given for texts essential to the following discussion.

(1) After launching the APP, the clerk first performs Arduino Bluetooth pairing. The clerk then enters and saves the following parameters: host server IP, customer code, and branch code (Fig. 5).

(2) Figure 6(a) shows that two of the five RFID cards are used to sense the tag code and then users should input a username/password. After a successful login, the user operates the Web POS 365 system. Figure 6(b) shows the details of the search result.

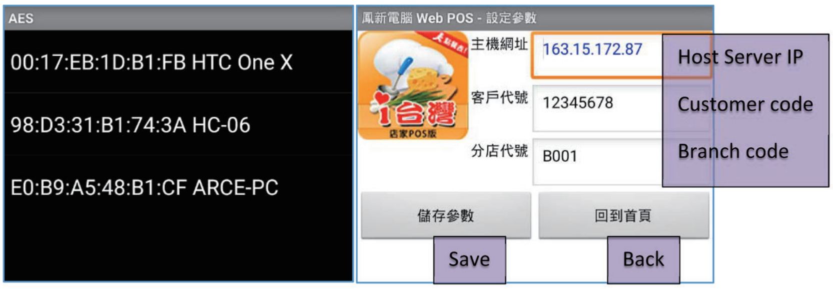
5. Security Analysis and Comparison

Since the original POS system uses one-factor authentication, the user can log in with only a username and a password. In our proposed scheme, not only the username and password are required but pin code, biometrics, and latitude and longitude information could be added. In other words, we can add parameters as needed.

Nevertheless, we use an RFID tag and (*k*, *n*) threshold authentication, and a user must have both an RFID card and a pin code to log in. In a (2, 5) threshold authentication scheme, for example, at least two of the five RFID cards and a pin code are required to log into the Cloud Web POS 365 Platform. That is, the authentication procedure is similar to that for the safe deposit box of a bank. The (1, 5) threshold authentication can also be used so that a single clerk can log into the platform.

Moreover, those parameters mentioned above are seeds to generate the key for symmetric encryption and decryption. In addition, the longitude and latitude are not only used as parameters, but are actually used for positioning. That is, the POS machine is set at the longitude and latitude of Taipei. If you take this POS machine to another place, such as Kaohsiung, then it cannot be used.

Via the deconstruction/reconstruction mechanism, the ciphertext is deconstructed into partial ciphertext segments and stored in a database. There is a secret channel to protect the



AES

00:17:EB:1D:B1:FB HTC One X

98:D3:31:B1:74:3A HC-06

E0:B9:A5:48:B1:CF ARCE-PC

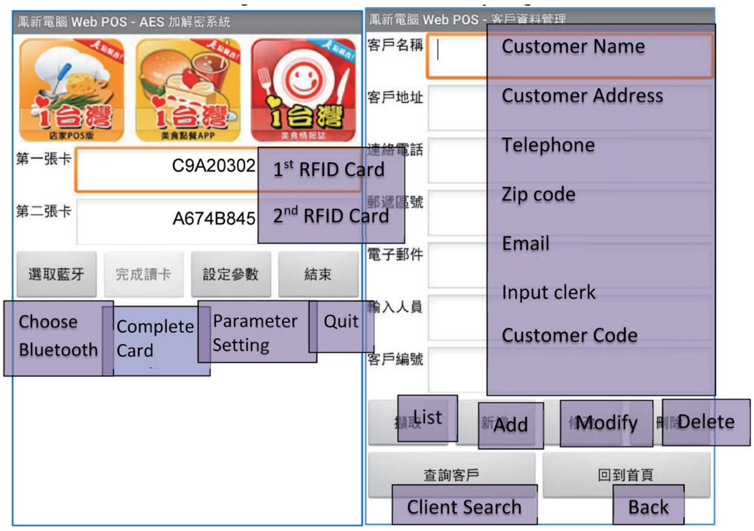
鳳新電腦 Web POS - 設定參數

主機網址 163.15.172.87

客戶代號 12345678

分店代號 B001

Fig. 5. (Color online) Arduino’s Bluetooth module pairing.



鳳新電腦 Web POS - AES 加解密系統

第一張卡 C9A20302

第二張卡 A674B845

鳳新電腦 Web POS - 客戶資料管理

(a) (b)

Fig. 6. (Color online) (a) RFID card tag code and (b) details of the search result.

transmission of a partial ciphertext; it is difficult for attackers to obtain one partial ciphertext database. Moreover, the attackers have to obtain a sufficient partial ciphertext database to restore the original ciphertext. Nevertheless, if the attackers obtain a sufficient partial ciphertext database, they must know how we deconstruct the original ciphertext. Even if the attackers know about our deconstruction algorithm, they have to know which bit comes from which partial ciphertext database.

In Fig. 3, raid 6 for example, there are 10! = 3628800 combinations to reconstruct the original ciphertext. In our scheme, the original or partial ciphertexts are still ciphertexts. This means that attackers have no plaintext-ciphertext pairs to analyze. Therefore, it is difficult for attackers to obtain the correct combination to reconstruct the original ciphertext.

As a result, it is difficult for malicious users to reconstruct the original ciphertext. Even though attackers reconstructed the original ciphertext, they have to have all of our parameters to obtain the decryption key or use brute force to crack the original ciphertext.

6. Discussion and Conclusions

In this study, we implemented the Cloud Web POS 365 Platform with a multifactor and threshold authentication. Then, we used the required and threshold parameters to generate a key for encryption/decryption. Finally, we deconstructed a ciphertext to partial ciphertext segments and stored it in each partial ciphertext database.

For convenience, Bluetooth connected the tablet and RFID reader. However, this connection is not currently secure. Since hackers can currently capture data transmitted by Bluetooth 2.1 to 4 at a distance of approximately 100 meters, data transmission would not be secure. The safest way to read an ID card would be to use a hardware security module (HSM),(17) which is very expensive. Therefore, the most practical approach would be to design a docking module that uses a micro-USB connection to connect the tablet computer to an RFID reader, which we will discuss in a future work.

One problem of a ciphertext format database is its low search efficiency. Creating an index for each record would greatly reduce search time, but the index collision problem should be solved. Until now, the searchable encryption is still an open question.

This study contains several security levels. First, users need the required parameters, including positioning information; when the machine is not in the set range, it cannot be used. Second, users need the threshold parameters stored in the RFID card and obtain enough card information to log into the system. Those parameters are the seeds used to generate the encryption/decryption key. Third, the symmetric encryption module (AES) is used to encrypt data. Fourth, the deconstruction/reconstruction module is designed to deconstruct and store a partial ciphertext in a separate database. Therefore, the proposed scheme is more secure than other cloud web POS systems. Moreover, its web-based architecture enables easy implementation in any platform.

In future works, we will design the RFID docking module to prevent wireless detection attack. In a searchable encryption problem, we have to design an efficient searchable encryption algorithm in the original ciphertext. However, how to search in a partial ciphertext database is still an open question that we hope some scholars can answer and solve.

Acknowledgments

This work was supported by the Ministry of Science and Technology, Taiwan under grant numbers MOST 108-2221-E-214-020, MOST 108-2221-E-037-007, and MOST 108-2218-E-992-304, by the “Intelligent Manufacturing Research Center” (iMRC) from the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan, by Kaohsiung Medical University under grant number KMU-M109007, and by the Taiwan Information Security Center at National Sun Yat-Sen University (TWISC@ NSYSU).

References

1 National Institute of Standards and Technology: FIPS 197, Advanced Encryption Standard (2001).

2 A. Shamir: Commun. ACM **22** (1979) 612.

3 V. Vishnu and P. Vinod: Int. Conf. Advances in Computing, Communications and Informatics (2016) 1694–1698.

4 M. Sajjad, S. Khana, T. Hussain, K. Muhammad, A. K. Sangaiah, A. Castiglione, C. Esposito, and S. W. Baik: Pattern Recognit. Lett. **126** (2019) 123.

5 R. W. John: US patent No. US9946858B2 (2018).

6 S. T. Dispensa: US patent No. US10122715B2 (2018).

7 J. Oberheide and D. Song: US patent No. US10440016B2 (2019).

8 R. A. Ford and B. L. Swafford: US patent No. US10326775B2 (2019).

9 M. Bellare and P. Rogaway: US patent No. 20180097624 A1 (2020).

10 M. Russell and H. Adam: US patent No. US20040058705A1 (2004).

11 Comodo Company: https://securebox.comodo.com/pos-system/pos-security (accessed 30 January 2020).

12 Ö. Cengiz and S. Erkay: Proc. 2012 Joint EDBT/ICDT Workshops (ACM, 2012) 186–195.

13 Z. Y. Xul, W. S. Kang, R. X. Li, K. C. Yow, and C. Z. Xu: IEEE 18th Int. Conf. Parallel and Distributed Systems (IEEE, 2012) 244–251.

14 A. P. Ashwini and L. Archana: Int. J. Sci. Eng. **3** (2018) 25.

15 T. Stephen: SSL and TLS Essentials (Wiley, Hoboken, 2000).

16 S. William: Cryptography and Network Security: Principles and Practice (Pearson, London, 2019) 8th ed.

17 National Institute of Standards and Technology: FIPS 140-2 IG, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (2019).