Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6233870, 7 pages
https://doi.org/10.1155/2022/6233870

Research Article

Computer Vision Operating System of Bank Economic Management Security under 5G Wireless Communication Technology

Guo Jianluan[1] **and Wang Xiaoyan**[1,2]

[1]*Business School, Central University of Finance and Economics, Beijing 100080, China*
[2]*Economics and Management School, Inner Mongolia University of Technology, Inner Mongolia 010051, China*

Correspondence should be addressed to Wang Xiaoyan; xiaoyanwang@imut.edu.cn

Received 18 January 2022; Revised 7 March 2022; Accepted 9 March 2022; Published 24 March 2022

Academic Editor: Kalidoss Rajakani

Copyright © 2022 Guo Jianluan and Wang Xiaoyan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Based on 5G wireless communication technology, this paper proposes a secure online banking payment scheme using a password algorithm and identity authentication+SMS verification code. We use the lightweight block cipher algorithm to construct a numeric permutation table. Then, we use the digital permutation table to perform the permutation encryption operation to obtain the digital ciphertext data. Finally, we connect 5G radiofrequency identification, identity authentication, and other modules to the trusted computing platform. The research found that the online banking security encryption algorithm proposed in the paper has the characteristics of high security and high efficiency.

1. Introduction

Online banking has developed rapidly under its unique advantages of convenience and low cost. At the same time, some criminals on the Internet took the opportunity to find new shortcuts to make a living. In the 5G era, the security problems of online banking have become more and more serious, and attackers have emerged one after another. Attackers mainly commit crimes by stealing online banking account passwords through Trojan horses and viruses [1]. They remotely control the "broiler" computer to transfer money directly. The thieves make full use of the bad usage habits of online banking users to steal funds from online banking user accounts. These problems cause varying degrees of financial loss to customers and damage the bank's reputation. According to the investigation by relevant departments, nearly 30% of users decided to reduce the use of online banking due to concerns about the safety of online banking after the infamous scene of online banking theft at the CCTV 3.15 party was exposed. All in all, online banking security issues are very important. It is the foundation of the bank's online banking business to strengthen the security construction of the online banking system and provide a relatively safe online banking operating environment for most users.

2. Security Analysis of Each Link of the Online Banking System

From the current cases in online banking, online banking cases are mainly divided into the following categories: hacker intrusion, Trojan horse virus, fake website, fake server, online banking information leakage, etc. Many experts and critics believe that the security awareness of online banking users is not high enough. The fundamental reason is that there are indeed loopholes in some aspects of the online banking system, allowing attackers to take advantage [2]. The online banking system mainly involves identity authentication and transaction processes. The system includes several main links such as client, data transmission, and online banking server system (Figure 1).

2.1. Bank Client. At present, the bank client is mainly threatened by the following aspects: (1) There are many vulnerabilities in the Windows operating system and its browser

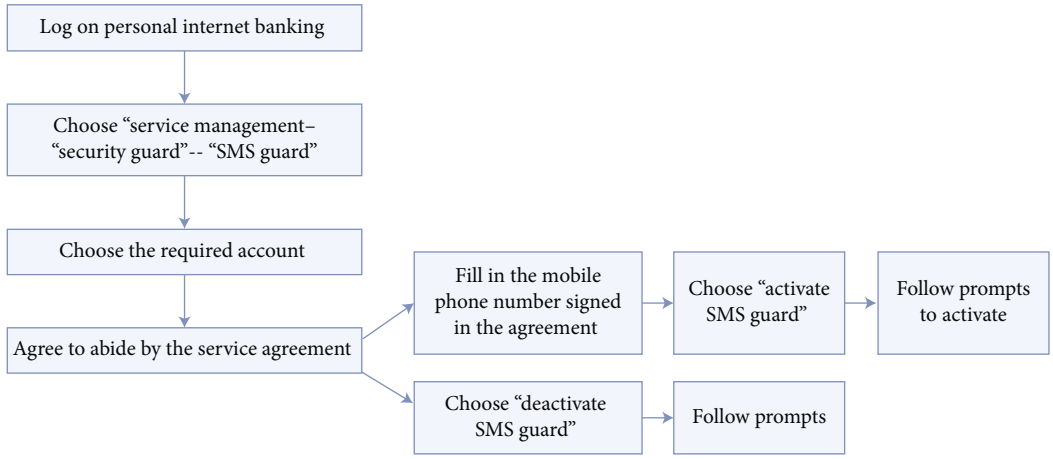

Figure 1: Online banking workflow.

commonly used by users. Customers with little awareness of prevention are prone to be hacked into the system with Trojan horses and viruses [3]. After the system is infected with Trojan horses or viruses, private information such as customer accounts and passwords will no longer be safe. (2) Some online banking customers are used to saving digital certificates on soft and hard disks. Once a Trojan is installed in the system, it is easy for hackers to copy the certificate, bank account number, and password together. This causes customers to suffer financial losses. (3) It is easy for users to be "phished" during the process of logging in to the page. Hackers often trick users into logging into a fake website that looks like a bank's official website and entering authentication information. Hackers indirectly obtain user authentication information in this way.

2.2. Online Banking Server System. Banks have done a lot to prevent attacks on their online banking server systems. First of all, most banks have built several firewalls between the Internet and online banking servers. This makes it impossible for hackers to break through the firewall and enter the bank's internal network. Secondly, the web application server-side uses a trusted, reliable operating system. With its unique architecture and security checks, the system ensures that only legitimate users' transaction requests can be sent to the application server for subsequent processing through a specific agent program.

Furthermore, banks mostly use international advanced network security detection and monitoring systems [4]. The system conducts 24 h real-time monitoring, alarming and blocking common operations in and out of local area networks at all levels. At the same time, the system regularly conducts security analysis on the network system to discover and correct vulnerabilities in time. The passwords used by customers in online banking are stored in the database through irreversible encryption algorithms. Even if hackers break into the database system, the original password cannot be deciphered. The online banking server system is more secure than the client after various layers of risk defense.

2.3. Data Transmission Process. Banks generally use 128-bit key SSL for secure encrypted communication transmission. The current commonly used version is SSL3.0. SSL3.0 realizes mutual authentication between browser and web server through digital signature and certificate. The verification method has the functions of confidentiality, message integrity, and freedom from replay attacks [5]. Although the protocol can provide security services such as encryption and authentication, it is not flawed. In recent years, SSL vulnerabilities have been exposed frequently. These security risks may expose users to various highly destructive network attacks. One of the most typical is the SSL man-in-the-middle attack. The sslstrip mentioned at the latest black hat conference is to deceive users and steal account passwords through man-in-the-middle attacks without changing the SSL encryption state. From this point of view, there is also a security risk in the data transmission process.

3. Technical Features and Defects of E-Token and USBKey Authentication

3.1. The Working Principle of E-Token and Its Technical Defects

3.1.1. The Working Principle of E-Token. E-token is a dynamic token of the size of a key. Inside is a built-in chip, clock, power supply, and an LCD window. It is a one-time dynamic password authentication technology (OTP) based on a time synchronization mechanism. The main idea is to add uncertainty to the login process. In this way, the password information transmitted for each login is different to increase identity authentication security. Banks establish a one-to-one correspondence with online banking users when distributing E-tokens. We initialize it with a unique 128-bit seed. Its internal chip changes a different algorithm every minute. Combine the seed with the current time to generate a random 6-digit number [6]. At present, the E-token distributed by the bank is updated with a dynamic password every 60 s. The authentication system on the bank side and the E-token on the client side have both the symmetric key and the same symmetric key algorithm. The system updates

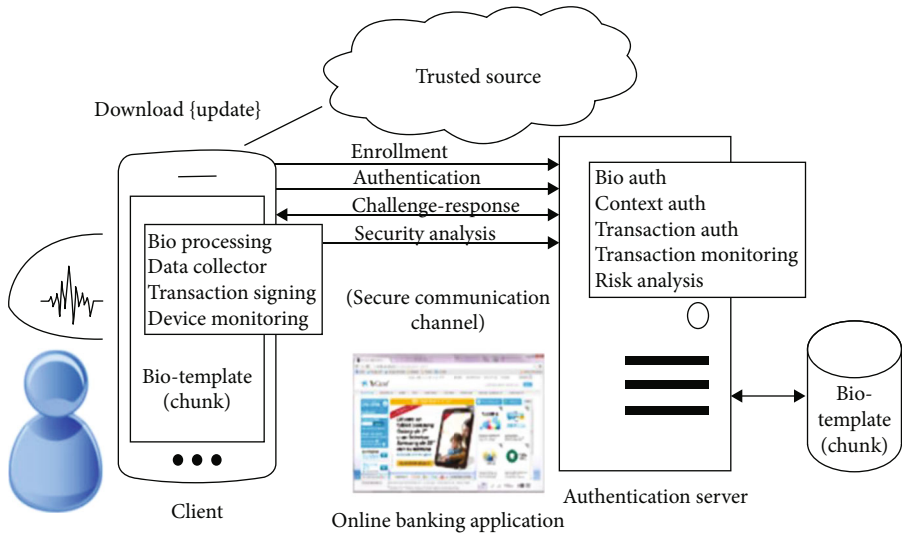

Figure 2: E-token-based online banking identity authentication and transaction process.

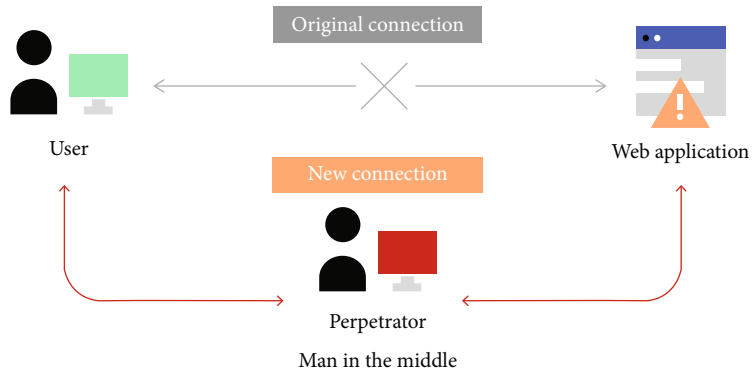

Figure 3: Illustration of a man-in-the-middle attack.

and calculates a new random number at the same set time. This ensures the single authentication of the dynamic port token and the online banking server to ensure online banking security. Figure 2 shows the login and transaction process of the online banking system using the E-token identity authentication technology.

3.1.2. E-Token Technical Defects. In just 60 s, the only possible way for an attacker to break through is to use MITM (man-in-the-middle attack). This intercepts user transfer operations and transmits login information, including OTP. Hackers pretend to be users and manipulate accounts at will. At this time, the online banking server cannot judge whether the user or the Trojan horse sent the transfer instruction [7]. Therefore, the online banking server executes the operation instruction impersonating the customer. It turns out that the man-in-the-middle real-time attack method is feasible. Hackers once successfully broke through the Citibank website through MITM and stole the accounts and passwords of Shanda Mibao and Netease General. The principle of man-in-the-middle attack is shown in Figure 3.

In addition, the OTP technology based on E-token does not support the electronic signature and public key calculation. It does not have the confidentiality, integrity, and nonrepudiation of information. The token can only provide one-way authentication and cannot prove whether the other party is indeed the authentication system on the bank side. Therefore, this secure encryption method is vulnerable to phishing. In early 2007, a hacker group invented a phishing tool and sold it online [8]. This tool can copy existing online banking pages and generate fake URLs. Phishing tools send back login information to hackers in real-time. Users will suffer economic losses if they are not careful.

3.2. The Working Principle of USBKey and Its Security Vulnerabilities

3.2.1. Working Principle of USBKey. Once a computer is hacked, the certificates and private keys on its hard drive can be stolen. USBKey is a hardware-based security technology that uses digital certificates for identity authentication.

USBKey is different from general U disk. It uses an IC card containing a CPU to store user certificates and private keys. The CPU has certain computer functions. It needs to enter a PIN code when using it. The smart card manufacturer burns the program for generating the public-private key pair and the cryptographic algorithm program in the ROM of the IC card chip [9]. The public key can be exported

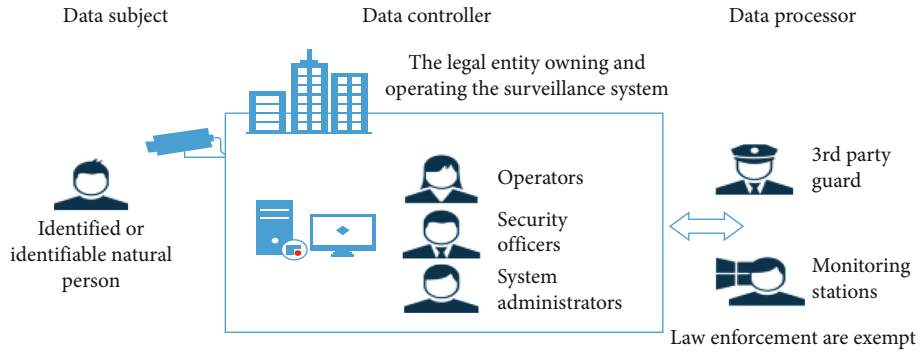

Figure 4: USBKey internal certificate and key working process.

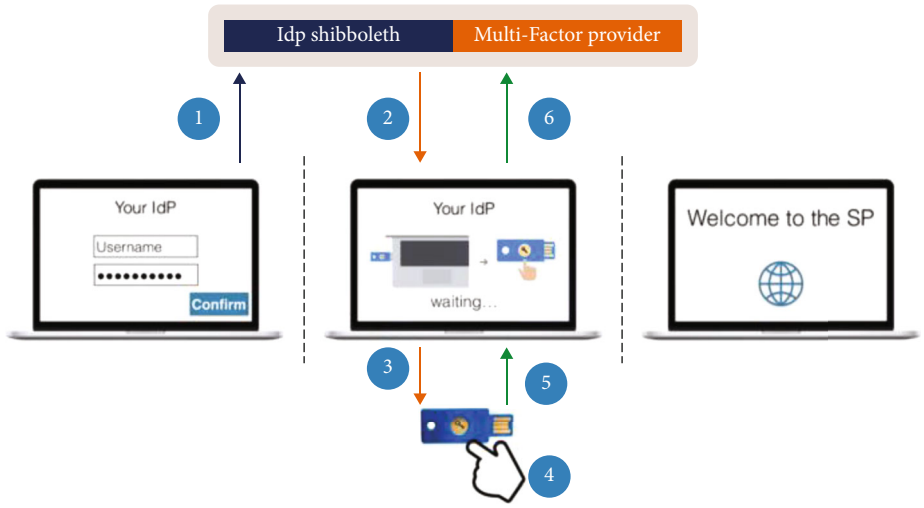

Figure 5: USBKey authentication process.

off the card. The private key is stored in the key area of the chip and does not allow external access. Online banking users are required to insert a USBKey when initiating business instructions. At this time, you also need to enter the corresponding PIN code. After successful verification, USBKey will digitally sign the business instruction to be sent. The system encrypts the signature with the original instruction with a randomly generated DES key and encrypts the DES key with the public key. Then, the system transmits the encrypted instruction, signature, and DES to the online banking server for verification by the other party.

The private key in the whole process can be out of the smart card medium [10]. At this point, there is no way for hackers to intercept the private key. This encryption method is safer than putting certificates and private keys on floppy or hard disks. The client USBKey workflow is shown in Figure 4. After receiving the client information, the online banking server uses its private key to decrypt the encrypted DES. Then, the client uses DES to decrypt the encrypted digital signature and instruction. The system then verifies the digital signature with the public key. This method can effectively prevent the instruction from being tampered with in the middle and ensure the nonrepudiation of the user's identity. The identity authentication process based on USBKey is shown in Figure 5.

3.2.2. USBKey Security Features and Its Defects. The security of the USBKey authentication method is that the USBKey adopts the PKI public key system. The digital certificate in it makes the transaction process relatively safe. And the digital certificate and private key in the USBKey are calculated and encrypted in the card. Hackers can never take out encrypted digital certificates. Furthermore, the existence of the PIN code can prevent the USBKey from being accidentally lost or stolen by others [11]. Although USBKey looks perfect, it has some security problems that OTP does not have. The USBKey authentication system has the following two loopholes: First, the hacker is fully capable of intercepting the static PIN code entered from the computer. When the user does not take out the USBKey in time, hackers can use the PIN code to obtain false authentication for transfer operations. The second is a security vacuum period after the user sends a transaction instruction and before the USBKey encrypts it. Hackers can tamper with user instructions silently at this time. The USBKey will also firmly protect the tampered instructions.

4. Improvement of Online Banking Identity Authentication Process

In the process of E-token authentication, the message integrity and nonrepudiation of USBKey technology are lacking.

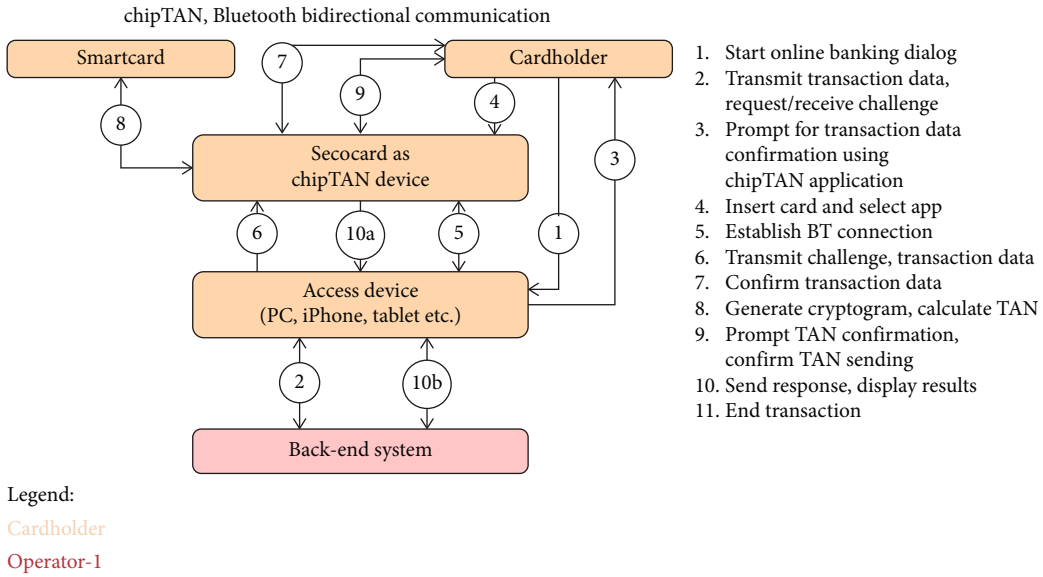

Figure 6: Improved online banking identity authentication communication process.

In the process of USBKey authentication, the static PIN code is easy to be used by hackers. This greatly reduces the entire online banking system [12]. Given the current situation of the online banking system, we combine the dynamic factors of E-token and the message integrity and nonrepudiation of USBKey to build a more robust online banking system. The improved online banking identity authentication process is shown in Figure 6. The improved online banking authentication process and encryption algorithm are as follows:

4.1. Round Key Plus Transformation. The round key plus transformation is a state and rk a one-to-one XOR operation:

$$F_2^{64} \longrightarrow F_2^{64}, \text{state} \longleftarrow \oplus rk^i, (1 \le i \le 32). \quad (1)$$

4.2. S-Box Conversion. S-box transformation is to divide state into 16 4b data. Every 4b of data undergoes a 4×4 S-box replacement operation.

$$F_2^4 \longrightarrow F_2^4, \text{state}_{j[3:0]} \longleftarrow S\left(\text{state}_{j[3:0]}\right), (0 \le j \le 15). \quad (2)$$

4.3. P Replacement. P permutation transformation is that state performs every 1b shift operation. Each bit of the permutation layer is permuted by the formula [13]. This operation does not consume resources in the hardware implementation process:

$$\begin{aligned} b_j &\longleftarrow b_{4\times j}, \\ b_{j+16} &\longleftarrow b_{4\times j+1}, \\ b_{j+32} &\longleftarrow b_{4\times j+2}, \\ b_{j+48} &\longleftarrow b_{4\times j+3}, (0 \le j \le 15). \end{aligned} \quad (3)$$

The structure of the round function is shown in Figure 7. The key expansion function is described in detail as follows.

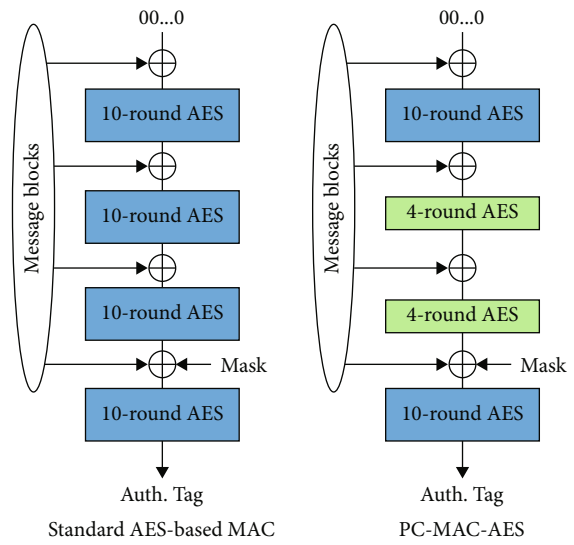

Figure 7: The round function structure of the PRESENT cipher.

Table 1: Attack analysis of PRESENT cipher.

Attack types	Rounds	Time	Data
MLC	26	272	266
TDC	26	276	263.16
FFT-MLC	27	274	262
BC	31	279.34	222

4.3.1. Cyclic Shift Transformation. The cyclic shift transformation is that k performs a cyclic shift 61b to the left:

$$k \longleftarrow k <<< 61. \quad (4)$$

4.3.2. Constant Plus Transformation. The constant plus transformation is k XORing a constant (round_count) for 5b rounds:

$$k \longleftarrow k \oplus \text{round\_count}. \tag{5}$$

The S-box in the key expansion and encryption round functions share the same S-box. The S-box replacement only replaces 4b in the 80b key once. The latest PRESENT cryptanalysis results are shown in Table 1.

The attack types in Table 1 include multidimensional linear attack (MLC), truncated differential attack (TDC), FFT-multidimensional linear attack (FFT-MLC), and Biclique attack (BC). The dataset of the plaintext message space numeric type is $X = 0.1, \cdots, 9$. We keep the ciphertext message dataset the same as the plaintext message dataset. The dataset of the permutation table constructed in the algorithm is also $X = 0.1, \cdots, 9$. The construction of an efficient and low-resource-oriented digital conformal encryption algorithm is implemented in six steps:

(1) Encrypt with Lightweight Block Cipher. We load 10 numbers from 0 to 9 into the register. At the same time, we use the lightweight block cipher to encrypt the 10 numbers with E_P operation. The lightweight block cipher key is k and the resulting tuple I:

$$I = (E_P(0, k), E_P(1, k), \cdots, E_P(9, k)), \tag{6}$$

where each component tuple $I_j = (E_P(j, k))(0 \le j \le 9)$. The length of these component tuples is the same as the block length of the lightweight block cipher algorithm. We generally take the value 64b.

(2) Tuple Data Sorting. We sort each component tuple $I_j = (E_P(j, k))$ in step 1 according to the size of binary numbers from high to low. In this way, a numeric permutation table sequence T is obtained.

(3) Add Plaintext, Modulo 10. We load the plaintext M into the register. M and the encryption key of the lightweight block cipher perform a one-to-one addition, modulo 10 operations:

$$(M + k) \bmod 10. \tag{7}$$

(4) Plaintext Encryption Replacement. We perform the permutation table permutation operation obtained in step 2 on the result data of the operation in step 3 to obtain the ciphertext C. This permutation is encrypted as E_T.

$$C = E_T((M + k) \bmod 10). \tag{8}$$

(5) Construct Inverse Permutation Table. Based on the positive permutation table, we construct an inverse permutation table for decrypting the ciphertext. The inverse permutation table is also a numeric permutation table sequence T^{-1}.

(6) Ciphertext Decryption Permutation. We first perform the inverse permutation table permutation operation on C. Then, we perform a one-to-one correspondence subtraction modulo 10 operation between C and the lightweight block cipher key to obtain M.

$$M = \left(E_{T-1}^{-1}(C) - k\right) \bmod 10. \tag{9}$$

5. Security Analysis of the Improved Online Banking Identity Authentication Process

The improved online banking identity authentication system requires reentering the dynamic PIN code every time the USBKey is used to encrypt the command. The system incorporates the uncertainty of E-token into the USBKey digital certificate. Compared with the system that uses E-token alone, the system adds the message integrity and antirepudiation functions of digital certificates. The improved authentication process draws on the strengths of the two current authentication technologies. The identity authentication encryption method greatly reduces the possibility of illegal transfer of users' online banking. At the same time, it significantly improves the security of the online banking system.

6. Conclusion

This paper analyses the entire workflow of the current online banking system. We believe that one of the security bottlenecks of the online banking system lies in the connection between the client and the data transmission. This connection is the online banking identity authentication process. We have investigated the two popular authentication technologies, USBKey and E-token. We combine the advantages of these two identity authentication technologies and propose a new online banking identity authentication scheme. The improved scheme combines the dynamic and uniqueness of E-token and the message integrity and nonrepudiation of USBKey to realize mutual authentication between client and server. It greatly reduces the risk of users being phished and attacked by a man-in-the-middle. At the same time, the scheme greatly improves the security of the online banking system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] K. K. Vaigandla and D. N. Venu, "A survey on future generation wireless communications-5G: multiple access techniques, physical layer security, beamforming approach," *Journal of*

Information and Computational Science, vol. 11, no. 9, pp. 449–474, 2021.

[2] R. Hussain, F. Hussain, S. Zeadally, and J. Lee, "On the adequacy of 5G security for vehicular ad hoc networks," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 32–39, 2021.

[3] Y. Huo, X. Dong, T. Lu, W. Xu, and M. Yuen, "Distributed and multilayer UAV networks for next-generation wireless communication and power transfer: a feasibility study," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7103–7115, 2019.

[4] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. Abd El-Latif, "A secure federated learning framework for 5G networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 24–31, 2020.

[5] P. Hong, Y. Kim, K. Cho, and S. Kim, "A study on security requirements for 5G base station," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 31, no. 5, pp. 919–939, 2021.

[6] Y. Qian, "5G wireless communication networks: challenges in security and privacy," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 2-3, 2020.

[7] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[8] K. Samdanis and T. Taleb, "The road beyond 5G: a vision and insight of the key technologies," *IEEE Network*, vol. 34, no. 2, pp. 135–141, 2020.

[9] A. S. Abdalla, K. Powell, V. Marojevic, and G. Geraci, "UAV-assisted attack prevention, detection, and recovery of 5G networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 40–47, 2020.

[10] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[11] G. A. Hussain and L. Audah, "BCH codes for 5G wireless communication systems over multipath fading channel," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 1, pp. 310–316, 2020.

[12] J. Chen, W. Wang, Y. Zhou, S. H. Ahmed, and W. Wei, "Exploiting 5G and blockchain for medical applications of drones," *IEEE Network*, vol. 35, no. 1, pp. 30–36, 2021.

[13] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 54, no. 9, pp. 1–37, 2022.