An Enhanced Design of the Identity Verification and Secret Communication Mechanism based on Smart Cards

Su, Pin-Chang Chen, Yue-Lin* Yang, Bo-Yuan

Department of Information Management, National Defense University, *Taiwan, R.O.C.*

Abstract

In modern society, nearly every aspect of modern life is performed in smart card-based remote connection environments, and this includes transportation, shopping, healthcare, home automation, and games. When clients remotely access a service, the information of service providers and clients may be stolen by malicious actors. Therefore, a session key must be constructed for both parties prior to the provision and usage of remote service. This key is subsequently used to mediate all exchange of information between these parties. However, when a single session key mediates all communications, the security of key becomes a matter of extraordinary importance. To improve the unpredictability of the session key, irrational numbers are often employed as parameters during bit-fetching processes in random number generation. In this work, we have proposed a highly elastic framework, which utilizes multiple irrational numbers to improve the security of encryption and decryption systems. The contributions of this research are as follows: (1) constructed a highly elastic encryption mechanism that meets the requirements of information security management. (2) improved the unpredictability of encryption and decryption system. (3) create a synchronous encryption system.

Keywords: Smart Cards, Identity Authentication, Secure Communication, Session Key

Relevance to National Defense: The system architecture proposed in this study can be applied to the National Military's current electronic document signature to prevent malicious user attacks, including fraudulent privileges, theft of smart cards and unlawful use of data, etc. In addition, because this research framework can be applied to the smart card identity verification mechanism in a multi-server environment, the organization is still reserved to integrate various services into smart card applications in addition to existing services.

* Corresponding Author: Chen, Yue-Lin email: tomleo795@gmail.com

植基於智慧卡之身分驗證暨秘密通訊機制創新設計

蘇品長 陳岳霖* 楊博元

國防大學資訊管理學系

論文編號：NM-44-01-10
DOI:10.29496/JNDM.202511_46(2).0003
來稿 2023 年 2 月 9 日→第一次修訂 2024 年 3 月 26 日→第二次修訂 2024 年 4 月 13 日→同意刊登 2024 年 5 月 22 日

摘要

現代生活舉凡交通、購物、醫療、智慧居家及遊戲等大小事，均於遠端連線環境下進行，為使參與者能夠合法的依照其權限存取服務，身分驗證在連線及溝通協議上扮演著重要的角色，而智慧卡由於其輕巧的特性及日益進步的晶片運算能力，於各領域中廣泛的被用於驗證機制，存取服務的秘密通訊過程中，會議金鑰是唯一溝通工具且分享於不安全的環境，易遭惡意行為者竊取。為此，本研究將設計可不透由網路並能使溝通雙方獲得會議金鑰的機制並採用無理數作為隨機取位參數，以達強化身分驗證暨秘密通訊之效果，本研究具體貢獻為：(1)建構符合資訊安全管理需求及具高彈性之加密機制；(2)改善及強化加解密系統之不可預測性；(3)使加解密系統具有同步性。

關鍵詞：智慧卡、身分驗證、秘密通訊、會議金鑰

國防相關應用：本研究所提之系統架構可應用於國軍現行電子公文簽署中，防止惡意使用者的攻擊手法，包含偽冒權限、智慧卡遭竊及其資料遭不法利用等疑慮，另因本研究架構可適用於多伺服器環境下之智慧卡身分驗證機制，故未來除現有的服務外仍保留組織可整合多樣服務於智慧卡應用之中。

*通訊作者：陳岳霖 email: tomleo795@gmail.com

1. Introduction

As internet speeds and smart phone penetration continue to rise with each passing day the amount of time being spent by the public on the internet is also rising accordingly. A plethora of services are continuously being introduced on the market to enhance user convenience. However, hacking methods are also being innovated and updated with unerring persistence, and cyberattack incidents are now occurring more frequently than ever. In this chapter, we will first explain the background and motivation of this research, describe our contributions, and finally illustrate the structure of this study.

In this age in which everything is linked to the internet, almost every aspect of our daily lives is facilitated by the internet. It has become evident that the Internet of Things (IoT) is gradually being brought to reality; for example, applications like e-commerce, smart homes, smart healthcare, and smart cities are now emerging rapidly like mushrooms after rain. All these applications are deeply reliant on inter-device connections via the internet. However, weaknesses in the security mechanisms of various website systems (especially e-commerce websites) has invited malware intrusions, which have led to the theft of sensitive user information like identity card numbers, birth dates, and credit card numbers. Ranganathan and Ganapathy (2002) have also noted that security and privacy concerns will directly affect the appetite of users for online shopping and negatively affect the development of e-commerce. Furthermore, smart home monitoring systems are frequently hacked by malicious parties owing to poorly configured settings or a lack of adequate security. Security is therefore an indisputable necessity in convenience-oriented applications. It is often said that "everything is nothing without security;" this is undoubtedly true in the field of information technology.

Although IoT applications are now beginning to take flight, the security of many services still remains in doubt. These convenience-oriented services therefore expose their users to a dangerous environment. A minor cyberattack incident may only result in a loss of information, but a severe incident could lead to losses of property. Also, there are many sensors built into the IoT structure, they have some limitations like low power, low storage, low memory, and low bandwidth. Therefore, the IoT-based system must face the problems of these limitations. In addition, since the devices in the IoT are connected in their respective environments, data must be transmitted through the Internet for communication. Therefore, the security of data transmission and the legality of the transmitter and recipient identity are one of the research priorities. The authentication protocol was first proposed by Lamport (1981) to perform identity legality authentication in an insecure environment using passwords and one-way encryption functions. A smart card is also a kind of IoT device. Due to its light weight and portability, it is widely carried or embedded in a portable device. However, because it is not fixed in a certain place and stores user sensitive information, the identity authentication architecture must prevent the leakage of confidential information caused by the theft or loss of the smart card.

Stream-cipher cryptosystems are computationally efficient and require only a small number of computations, which makes these systems highly suited for devices like mobile devices or smart cards. However, the protection of the stream-cipher key is crucial for the security of the overall system. After the session key is generated, the scrambling is performed to improve the security, and the irrational number with infinite length and the number of non-repetitive characteristics is selected as a parameter, and the multi-irrational number is added in the scrambling phase to make the system selective and unpredictable.

In addition to security vulnerabilities, managing a large number of smart cards also faces challenges in terms of efficiency and accuracy. Effectively managing, updating, and revoking permissions and keys of smart cards has become a crucial task for administrators (Datta et al., 2020). To enhance management efficiency, allowing both communicating parties to directly obtain session keys without the need for network transmission can significantly improve

efficiency and accuracy in management. Furthermore, the synchronization of encryption systems can also bolster management efficiency by ensuring consistency among various smart cards.

This study aims to design a model for session key bit-fetching and scrambling to enhance the security of identity authentication. The contributions of this study are as follows:

- Introducing selectable scrambling parameters at the bit-fetching and scrambling stages, aiming to elevate post-scrambling complexity and enhance the difficulty of cracking the system.
- Systematically providing and designing multiple unpredictable bit-fetching parameters, enabling encryption via the selection of variable parameters, thus enhancing security measures.
- Designing a method enabling synchronous transmission and reception, which improves operational efficiency by facilitating direct access to the conference key without reliance on network transmission, consequently enhancing management accuracy and ensuring consistency across various smart cards.

In this section, the motivation, and contributions of this study and its structure are introduced and described to allow the reader to gain a preliminary understanding of this paper. In Section 2 we review the fields and techniques related to this study. These techniques and means of security are the focus of this paper and described in Sections 3 and 4. Section 5 provides the research conclusion.

2. Related Works

In this section, we review the literature studies relevant to this work, discuss the research on IoT security, identity verification, and furthermore propose the research objective and the architecture of the identity verification process. This section will help understand the operation of the current mechanism.

2.1 Introduction to IoT Security

When it comes to IoT security, we face a series of serious and diverse challenges. One of the main issues is that many IoT devices have weak default authentication, providing a vulnerability for hackers to attack (Schiller et al., 2022). For example, the Mirai botnet attack used these weak authentications to infect multiple devices and then launched a distributed denial of service (DDoS) attack, paralyzing important network services. Although the IoT brings huge economic benefits and the emphasis on IoT security continues to increase, the actual situation shows that the IoT industry and its devices still have many shortcomings in terms of security.

In addition, since users and devices in the IoT environment need to establish two-way communication, there is mutual communication between the device and the server. The device will send data to the server and receive control data sent by the server. Therefore, in IoT systems, mutual authentication is crucial to check the validity of devices and servers, and there is a huge demand for lightweight authentication and encryption (Hassan, 2019).

2.2 Stream Cipher

A stream cipher is a symmetric encryption algorithm that encrypts and decrypts a symbol, a character, or a bit at a time. The concept of stream encryption is to use a character in plaintext and generate a corresponding character of the ciphertext (Yu et al., 2022). To achieve stream-cipher encryption in situations where the length of the key is insufficient, it is necessary to design a mechanism to extend the key, thus generating a keystream that is long enough to cover the entirety of the plaintext; the ciphertext is then generated by performing an operation between the keystream and plaintext. However, the parties who are performing encryption and decryption operations using this system are both reliant on a "synchronous" mechanism, which

ensures that both parties may then use the same model to operate on the same document. The encryption and decryption procedures of stream-cipher encryption are shown in Figure 1.

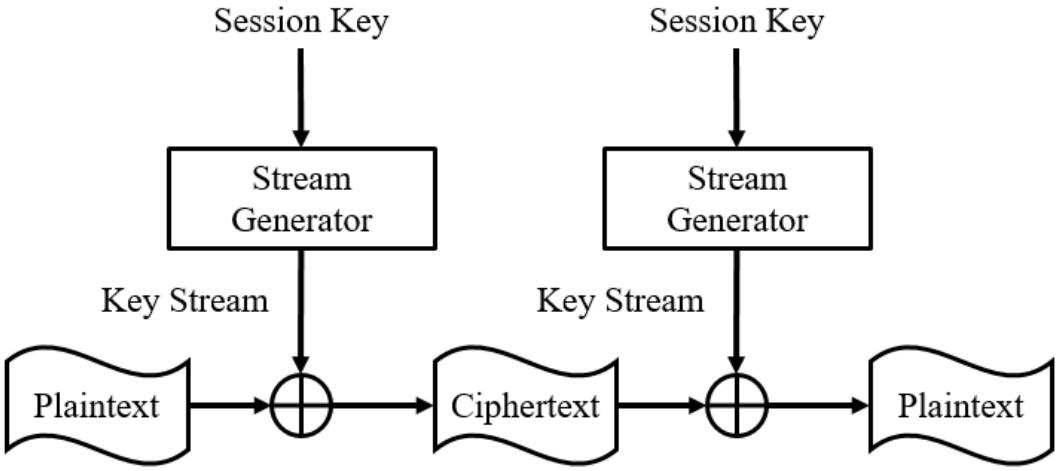

Figure 1 The encryption and decryption procedures of stream-cipher encryption

2.3 Session Key

In symmetric encryption systems, encryption is performed using only a single session key by the parties who are transmitting and receiving a document. Rafaeli and Hutchison (2003) divided session key management architectures and their modes of operation into the three following categories:

- Centralized group key management protocols:
  This method of management only uses a single key distribution center (KDC); in other words, key management does not require additional user or server resources during communication processes. This reduces the consumption of user and server-side operational resources by encryption processes and increases the overall computational efficiency of the framework.
- Decentralized key management architectures:
  As compared to centralized group key management protocols, this protocol divides a system into different groups; key management is then made the responsibility of each subgroup.
- Distributed key management protocols:

In this protocol, a KDC does not exist as the keys are independently calculated and generated by members of the system.

2.4 Linear Feedback Shift Register (LFSR)

As the communications of symmetric encryption systems rely on a single key, it is necessary to encrypt the key to produce a keystream before the key may be transmitted via an unsecure network. Besides scrambling and obfuscation, a key may also be encrypted through its input into a shift register; the key then acts like a seed sequence for generating a set of random sequences. However, the size of the sequence's periodicity will determine the security of the encryption mechanism. Therefore, linear functions are added to the shift register to form a linear feedback shift register (LFSR), which generates a random sequence from a seed sequence within 2^m-1 cycles (with m being the highest power of the linear function). Menezes et al. (2003) also noted that LFSRs are able to produce random sequences with large periodicities, and they are well-suited for hardware implementations. Therefore, LFSRs are used in many keystream generators.

2.5 Identity Authentication

The architecture of identity authentication was first proposed by Lamport (1981) to

implement a password-based identity authentication mechanism in an insecure network environment. Many studies on identity authentication mechanisms have been proposed. Huang and Li (2000) proposed a new remote user identity authentication architecture based on smart cards, which uses the discrete logarithm-based public key encryption technology proposed by Elgamal (1985). The architecture does not require the use of a password table in order to prevent an intruder from modifying the password stored in the system.

In 2009, Liao and Wang (2009) proposed a user identity authentication scheme for multi-server environments and claimed that its scheme can withstand many possible attacks. Hsiang and Shih (2009) pointed out that Liao and Wang (2009) could not defend against insider attack, masquerade attack and poor reparability and could not provide mutual authentication and proposed new user authentication scheme for multi-server environments to complement these shortcomings. In 2011, Sood et al. (2011) found that the architecture proposed by Hsiang and Shih (2009) is vulnerable to replay attack, impersonation attack, and stolen smart card attack. Moreover, the password changes phase of Hsiang and Shih 's protocol (2009) is incorrect. Lee et al. (2011) also found that the architecture proposed by Hsiang and Shih (2009) is still vulnerable to a masquerade attack, server spoofing attack, and is not easily reparable. Sood et al. (2011) and Lee et al. (2011) propose a solution based on the above problems. However, the proposed architecture is still proven to have many weaknesses. In 2014, Xue et al. (2014) pointed out that Li et al. (2012) proposed authentication scheme cannot resist replay attack, Denial-of-Service attack, smart card forgery attack and eavesdropping attack. Xue et al. (2014) apply timestamp to the proposed architecture. In the same year, Lo (2014) found that the protocol proposed by Li et al. (2012) does not adequately manage the rights of logged in users, which may lead to the arbitrary theft of sensitive information by unrestricted and restricted users alike Amin et al. (2018) proposed a lightweight identity verification architecture based on IoT devices and pointed out that Xue et al. (2014) and Chuang and Chen (2014) have security weaknesses. Jangirala et al. (2017) show that Shunmuganathan et al.'s scheme (2015) is defenseless in resisting the password guessing attack, stolen smart card attack, user impersonation attack, forgery attack, forward secrecy, and session key secrecy.

3. The Proposed Protocol

In this study, the proposed protocol has the addition of multiple irrational numbers to the bit-fetching and scrambling phases to increase the abilities of anti-attack and the security of the encryption system. The protocol itself is divided into five phases: the registration phase, the login phase, the identity authentication and session key generation phase, session key scrambling and extension phase, encryption and decryption phase. The operational context diagram of the proposed protocol is shown in Figure 2 and Table 1 lists the notations and its meanings which is used in this protocol.

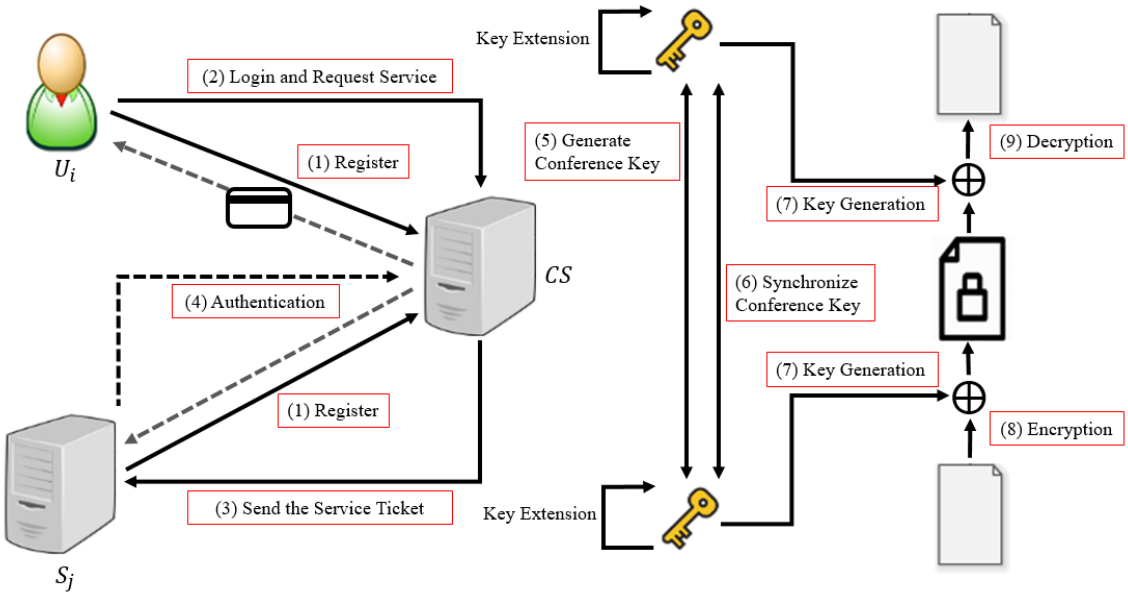

Figure 2 The operation context diagram of the proposed protocol

Table 1 Notations and their meanings

Notations	Description
U_i	User
S_j	Service providing server
CS	Control server
ID_i	Identity of U_i
CID_i	Identity generated dynamically during U_i
P_i	U_i's password
SID_j	Identity of the service provider server S_j
SID_{CS}	Identity of the control server CS
b	Random parameters generated by U_i (stores in the smart card)
N_{i1}	Random parameters generated by Ui 's smart card
N_{i2}	Random parameters generated by S_j
N_{i3}	Random parameters generated by CS
x, y	Random parameters generated by CS
SK	Session key
SK_{len}	Length of the session key
P_n	The number of bit-fetching parameters provider by the system
i	Irrational number
$h(.)$	Hash operation
$\oplus$	XOR (Exclusive-OR operation)
$\|$	Message concatenation operation

3.1 Registration Phase

In this phase, as indicated in step 1 of the Figure 2, all the roles of the system are registered with control server CS respectively. First S_j send $\mathrm{SID_j}$ to CS as the registration request. After receiving the request, CS selects two random parameters: x 、y and performs two operations like $h(SID_j||\mathrm{y})$ and $h(x||y)$. Then CS sends the result of operations back to S_j.

User (U_i) sends identity (ID_i) and $A_i = h(b||P_i)$ to the CS for registration after it selects ID_i, password (P_i), and random parameter (b). When CS receives ID_i and A_i, it calculates B_i, C_i, D_i, E_i, W_{ij}, then stores (C_i, D_i, E_i, W_{ij},$h(y)$,$h(.)$) in smart card. The smart card must be handed over to U_i via a secure way in real world. Then U_i stores b in smart card after receiving it. Now smart card stores (C_i , D_i , E_i , W_{ij} , $h(y)$, $h(.)$, b). The procedures of Registration phase are shown in Figure 3.

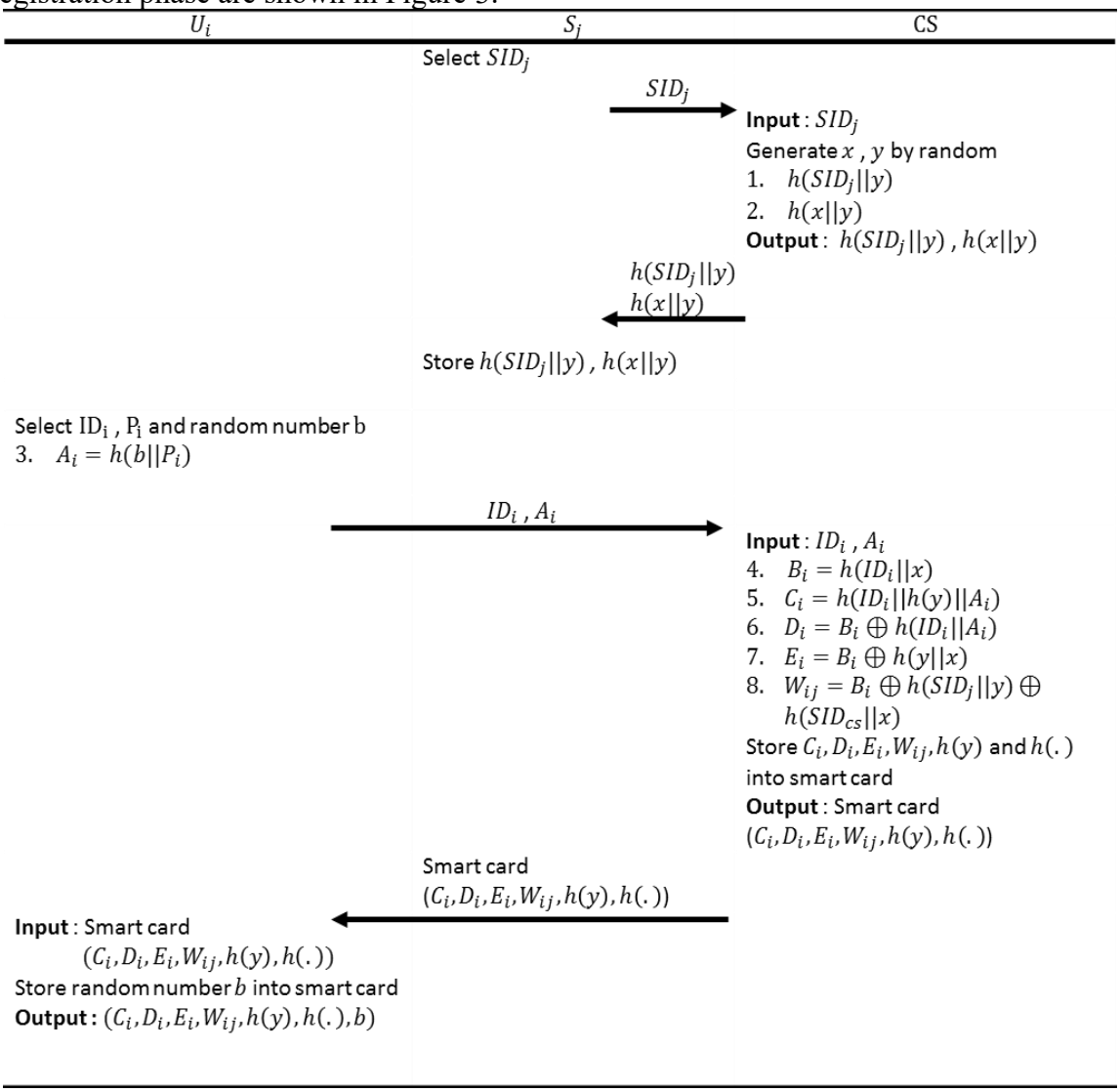

Figure 3 Registration phase of the proposed protocol

3.2 Login Phase

In the login phase, as indicated in step 2 and 3 of the Figure 2, verification of user legitimacy by the parameters stored by the smart card itself. The procedure for the login phase is depicted in Figure 3 Firstly, user U_i inserts his/her smart card into a terminal. After U_i input ID_i, P_i and the random parameter b, smart card calculating A_i by b and P_i. Then using A_i, P_i, $h(y)$ operation to obtain C_i'. The smart card then checks whether the original C_i stored in itself and the computed one C_i' are equal. If they are unequal, the user did not input the correct information and the login process is aborted. If these verifications succeed, smart card then

generates a random number N_{i1} and computes B_i, F_i, P_{ij}, CID_i, G_i. Finally, send $(F_i, G_i, P_i, W_{ij}, CID_i)$ to control server CS. The procedures of Login phase are shown in Figure 4.

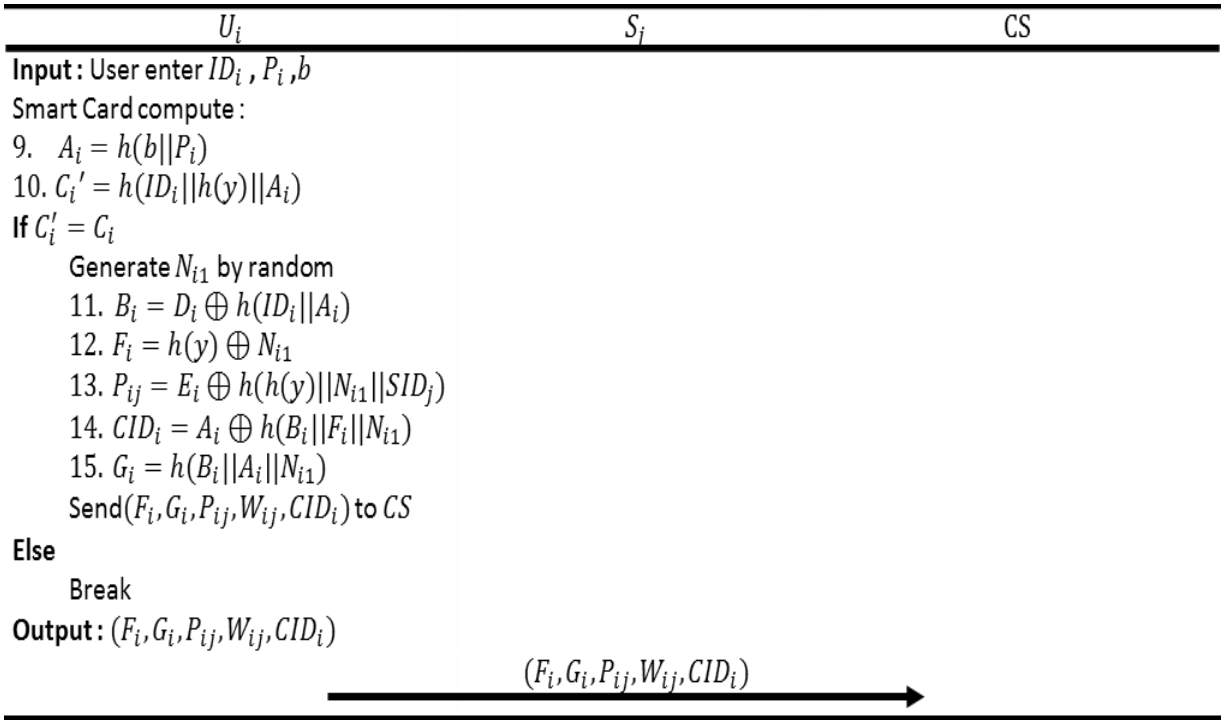

Figure 4 Login phase of the protocol

3.3 Identity Authentication and Session Key Generation

In the identity authentication and session key generation phase, as indicated in step 4 to 6 of the Figure 2, CS received $(F_i,\ G_i, P_{ij},\ W_{ij},\ CID_i)$, a series of operations will be performed to verify and generate the session key. The procedure for this phase is depicted in Figure 4. The verification method is to check whether the G_i' obtained by the operations and the received one G_i are equal. If they are equal, the verification is successful. Then CS sends service ticket W_{ij} to the service providing server S_j that the user U_i wants to apply for.

When receiving the ticket W_{ij}, S_j generates a random number N_{i2} and computes K_i,M_i and then sends them back to CS. CS computes M_i', W_{ij}' and checks whether M_i', W_{ij}' and M_i, W_{ij} are equal respectively. If they are equal, CS generates a random number N_{i3} and computes Q_i, R_i, V_i, T_i and then sends them to S_j.

After receiving $(Q_i,\ R_i,\ V_i,\ T_i)$, S_j computes V_i' by and then checks whether the V_i and V_i' are equal. If they are equal, S_j sends V_i, T_i to user U_i. Then U_i computes V_i' and then checks whether the V_i and V_i' are equal. If they are equal, the session key of communication is SK. The procedures of Identity authentication and session key generation phase are shown in Figure 5.

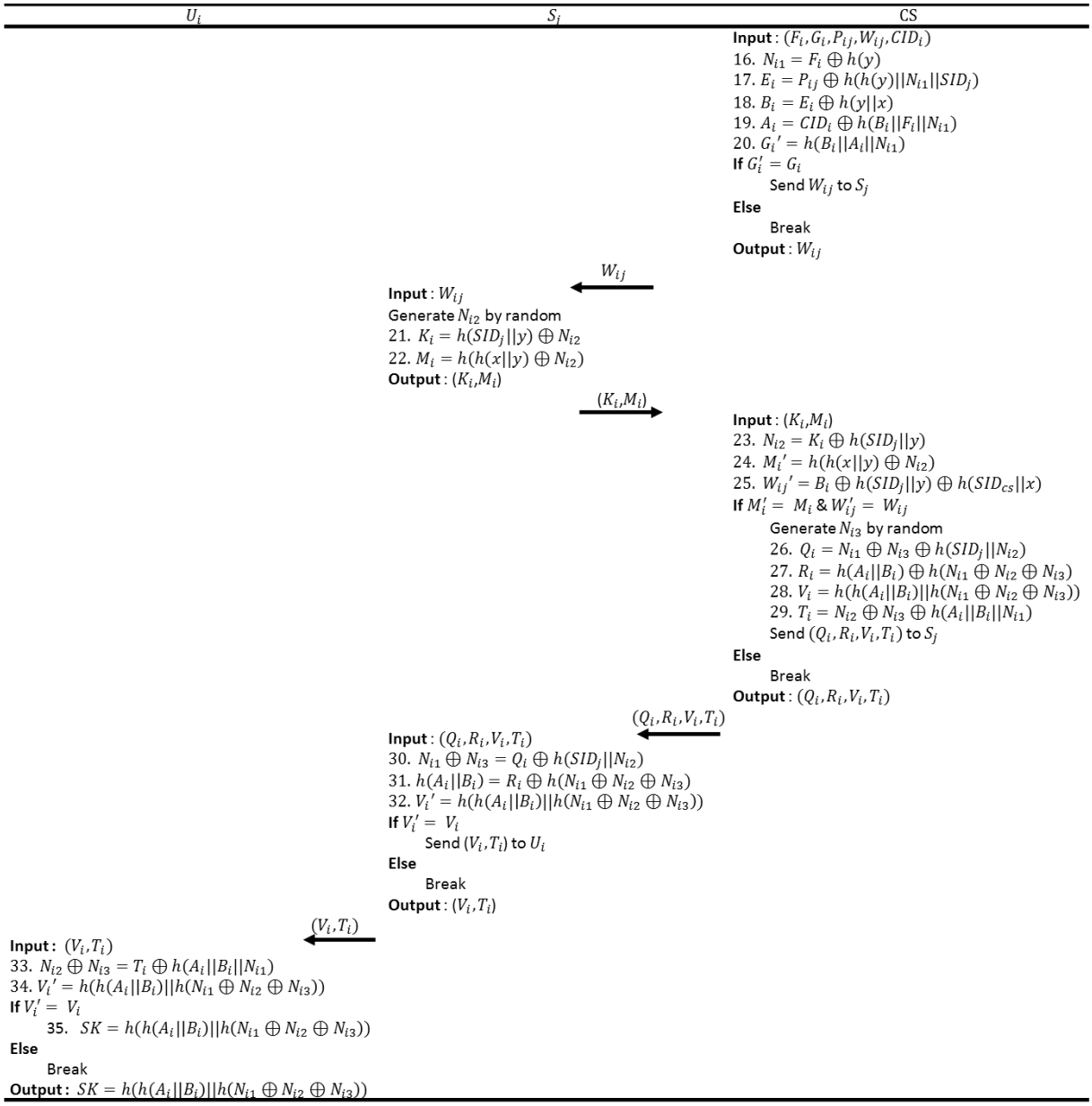

Figure 5 Identity authentication and session key generation phase

3.4 Session Key Scrambling and Extension Phase

In the session key scrambling and extension phase, as indicated in step 7 to 9 of the Figure 2, our research proposed the secret communication scheme with multiple selections, the core of this scheme is to import multiple bit-fetching parameters. This phase is divided into three operations: bit-fetching and scrambling, key extension, and encryption/decryption. The operations of this phase are as follows:

3.4.1 Bit-fetching and Scrambling

Before the bit-fetching, the system provides the irrational number sets $INum$ and randomly gives the serial number of the elements. Then performs the operation to obtain the random number that length is equal to the session key SK. Finally, an XOR operation is performed between the random number and the session key SK. The procedure for the bit-fetching and scrambling is depicted in Figure 6. The steps of operation are as follows:

Step 1. Transfer the session key to decimal form: The input session key has been operated by the hash function to be shown in hex form, so the first step is to make the hex session key transfer to decimal form.

Step 2. Decide on the number of bit-fetching parameters to use: A modulo operation is

performed between the result of step 1 (n) and the number of bit-fetching parameters provided by the system (P_n). Then we will get the number of bit-fetching parameters in this phase (n').

Step 3. Select bit-fetching parameters: Select parameter number 1 to n' in the $INum$ sets to integrate a new set ($INum\_selected$).

Step 4. Decide on the bit-fetching value: Perform a modulo operation between the sum of every bit in session key SK and P_n to obtain the bit-fetching value tb.

Step 5. Bit-fetching: Among all the parameters of the parameter set $INum$, the number of SK_{len}/n' bits is fetched from the tb-th bit of each parameter, and is combined into a random number p according to the execution order.

Step 6. Scrambling: Perform an XOR operation between the random number p and session key SK

Algorithm 1. Bit-fetching and Scrambling

Input : Session key SK

The system provides the irrational number sets $INum$ and randomly gives the serial number of the elements.

BEGIN

$n = toDecimal(SK)$

$n' = (n \bmod P_n) + 1$

$INum_$selected $= \{i | i \in irrational\ number\}$

For s in SK:

$sum \mathrel{+}= s$

$tb = sum \bmod P_n$

End For

For i in $INum_$selected:

$p \mathrel{+}= substring(i, tb, SK_{len}/n')$

End For

$pSK = p \oplus SK$

END

Output : pSK

Figure 6 Bit-fetching and scrambling

3.4.2 Key Extension

In order to comply with the characteristics of streaming cipher, after the scrambled session key (pSK) is obtained, it must be increased to facilitate subsequent calculation with the file. In this research, pSK is imported into the LFSR, so that the highest power of the linear function is the length of pSK (m), the function is expressed as follows:

$$P(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0 \tag{1}$$

The sequences produced after importing pSK into P(x) is expressed as follows:

$$s_i = s_{i-1}s_{i-2} \ldots s_0 \tag{2}$$

3.4.3 Encryption and Decryption

The encryption phase XORs the message based on the element and key stream, while the decryption phase operates in reverse, as shown below:

$$M = m_1, m_2, m_3, \ldots, m_i \tag{3}$$

$$c_1 = m_1 \oplus s_1, c_2 = m_2 \oplus s_2, \ldots, c_i = m_i \oplus s_i \tag{4}$$

$$C = c_1, c_2, c_3, \ldots, c_i \tag{5}$$

4. Security Analysis

Our research imports irrational numbers into the identity authentication and secret communication system. In order to assure the safety of the proposed scheme, we will follow two famous international standards. First, ISO's requirements for information safety management, such as access control safety, service availability, and confidentiality. Second, the NIST authentication and secret communication authentication for mechanisms; against the replay attack, impersonation attack, authentication shortfall attack, and stolen card attack. Finally, we will focus on the three main feature of the stream cipher mechanism: high-elasticity, unpredictability, synchronization. The following descriptions explain the intended purposes:

4.1 Access Control

Access control plays the role of assigning system resources and access rights in the system. Its importance lies in judging the legitimacy of using system resources through the authentication mechanism. The network environment covers many users and service servers. Access control is like the concept of pairing, different services are sent to different users according to the request, and the service server must also join the verification mechanism to determine the legitimacy of the user. The scheme proposed in this study is implemented in $W_{ij} = B_i \eth h(SID_j \| y) \eth h(SID_{cs} \| x)$ The CS verifies whether the tickets W_{ij} are equal to confirm the legitimacy of the user and the service server, so the proposed scheme can meet the access control requirements.

4.2 Service Availability

The service availability is defined in the RFC2828 as "a security service that protects a system to ensure its availability." Under the system architecture consisting of users and servers, the attack mode that will influence the service availability can continuously transmit packets to the service server. It will cause the packet congestion, which in turn affects the service availability.

The system design is similar to Kerberos. When the user wants to use the service provided by the service server, the user has to obtain the authentication and an authorization through the control server before entering the server legally. The user will obtain the service ticket $W_{ij} = B_i \eth h(SID_j \| y) \eth h(SID_{cs} \| x)$ from the control server during the registration phase. The authorization code $P_{ij} = E_i \eth h(h(y) \| N_{i1} \| SID_j)$ will then be calculated by the smart card in the login phase. The user must send these two parameters to the control server for verification before using the service. If the ticket received by control server dose no contain the above two parameters. It is considered as an illegal request. This mechanism can effectively resist the denial-of-service attack and maintain system availability.

4.3 Confidentiality

The purpose of confidentiality is to protect information from unauthorized disclosure. For example, sensitive data such as revenue data or customer information in the company can only be accessed by authorized persons such as senior executives and sales departments. Other departments should not take it. Stream cipher can be used to encrypt a large number of data streams, and it has the characteristics of fast computation speed and can be applied to devices with constrained computation. In this study, the irrational number sets are used to generate the random number. Through transposition and disturbance, the length of the session key is increased and the difficulty of guessing the key is also increased. Therefore, the scheme proposed in this study can meet the requirements of confidentiality.

4.4 Resist Replay Attack

A replay attack is an attack that transmits the same data in different authentication phase to pass the verification. The attacker steals the password or the hash value used in the authentication phase by both two parties of verification. After obtaining the above values, the attacker will send these values to try to pass another authentication phase. The proposed scheme

generates random numbers (N_{i1}, N_{i2}, N_{i3}) to implement the resistant of replay attack in the different phase: $F_i = \mathrm{h(y)} \oplus N_{i1}$ 、$K_i = h(SID_j||y) \oplus N_{i2}$ 、$Q_i = N_{i1} \oplus N_{i3} \oplus h(SID_j||N_{i2})$.

By the characteristics of the hash function and generating random numbers at the different phase, the attacker cannot use the hash value in the next time. Therefore, the scheme proposed in this study can effectively resist the replay attack.

4.5 Resist Impersonation Attack

An attacker who launches an impersonation attack spoofs a channel in the network that the communication parties in the system consider to be secure, and then obtains information from it and pretends to be a legitimate user through the authentication mechanism. For example, when a customer contacts the e-commerce store, the attacker can pretend as the boss and get some private information from the customer. If there is no mechanism to resist the impersonation attack in the authentication scheme, and the system is easily cracked by the attacker.

In the proposed scheme of this study, the user must send ($F_i, G_i, P_{ij}, W_{ij}, CID_i$) to control server to CS. The attacker can not compute $P_{ij} = E_i \oplus \mathrm{h}(B_i||F_i||N_{i1})$, $G_i = h(B_i||A_i||N_{i1})$. Also, the $A_i = h(b||P_i)$, $h(ID_i||A_i)$cannot be computed by attacker. In summary, the authentication scheme proposed in this study can defend against impersonation attacks.

4.6 Resist Leak-of- verifier Attack

In the authentication scheme, the user will enter their personal information to log in (such as ID and password, etc.). If this information does not be encrypted during the authentication, it will make the attacker get user's sensitive information easily. The common methods just like the SQL Injection and XXS (Cross-Site Scripting) mentioned by OWASP (Wichers and Williams, 2017). They are aimed at stealing sensitive information stored in the server, and then obtain a legal identity login system. The authentication scheme proposed by this study does not store the sensitive information in the server so the attacker cannot obtain it through the server. Moreover, the system combines the user account and the password with the random number and then performs the hash operation. Even if the attacker obtains the hash value, the ID and password will not be known.

4.7 Resist Stolen Smart Card Attack

When the smart card is lost or stolen, the attacker can obtain the stored information and use the acquired data to infer the user's sensitive information. Therefore, when designing the authentication scheme, user information must be protected by a specific mechanism to prevent it from being easily obtained after they fall into the hands of malicious people.

The scheme proposed in this study uses random numbers to protect user information from malicious actors. identity and passwordP_i. When the user's smart card is lost or stolen, the attacker obtains the information in the smart card. Because the attacker cannot know the random number x, y generated by the control serverCS, it cannot guess ID_i and P_i, it is also impossible to calculate $A_i = h(b||P_i)$ and $B_i = \mathrm{h}(ID||x)$ by information stored in the smart card to launch an impersonation attack.

4.8 High-elasticity

Information security incidents now occur more frequently than ever before. Even if new encryption algorithms continue to evolve, the challenge of malicious attacks is inevitable. Our research imports the concept of elasticity to the encryption algorithm, which is to make the system difficult to be broken by a single method or a large number of operation attack.

Our research imports the irrational number sets $INum$to make the system select the parameters more elastic in the follow-up phase.

4.9 Unpredictability

In the stream cipher, the session key is the only one tool to communicate. To avoid stealing session keys when they are transmitted in an insecure network environment, it's important to make sure the process of dealing session key is random and to prevent an attacker from breaking

the secret in a valid time.

In order to achieve the unpredictability of the system, in the bit-fetching and scrambling phase, our research gives the serial number of the parameters randomly in the irrational number sets to achieve the propose of unpredictability.

4.10 Synchronization

Since the stream encryption system uses only one session key for communication, the recipient and the sender of the file must be able to obtain the same result even if they perform the operation at the phase of determining the parameter and the bit value, and there is no possibility of transmitting and receiving in the process of scrambling the session key.

4.11 Comparison with Related Schemes

In this section, we discuss the performance of the proposed scheme in terms of security property. We can see that Shunmuganathan et al. (2015) and Jangirala et al.'s scheme (2017) cannot resist impersonation Attack or stolen smart card attack. Amin et al.'s scheme Inability to achieve high elasticity and unpredictability. In Table 2, we present and compare security properties of the listed authentication schemes.

Table 2 Comparison analysis of the proposed scheme with other existing methods in terms of security measures

Comparative project	Shunmuganathan et al. (2015)	Jangirala et al. (2017)	Amin et al. (2018)	Our Scheme
Access Control	×	×	○	○
Service Availability	○	○	○	○
Confidentiality	○	○	○	○
Resist Impersonation Attack	×	○	○	○
Resist Leak-of verifier Attack	○	○	○	○
Resist Stolen Smart Card Attack	×	○	○	○
High-elasticity	×	×	×	○
Unpredictability	×	×	×	○
Synchronization	○	○	×	○

5. Conclusion

In this work, we have introduced the concept of high elasticity and incorporated it concept in the selection of scrambling parameters. This helps to improve the overall resistance of the system against malicious attacks, while consuming only a small amount of computational resources for stream-cipher encryption. At present, end devices in IoT and cloud computing tend to be relatively light and lacking in computational resources. Therefore, encryption systems that are computationally efficient have unlimited prospects for development. The contributions of this work are as follows: we have (1) improved the unpredictability of encryption of decryption systems, (2) created a highly elastic encryption mechanism that satisfies the security requirements of information management applications, and (3) produced a synchronous encryption system.

5.1 Applications to National Defense

Because of the sensitivity and special nature of data in the military, and the organization type is divided into different classes, each class of users oversees different authority. The identity verification mechanism of the smart card must play a key role in the application of the

national military.

At this stage, smart cards are used in many ways. The use of smart cards in electronic document signing, including the different approval authority of various levels of officers, has gradually led to the use of electronic forms for document approval. By inserting the smart card and entering the account number and password, the user can perform the operations belonging to his authority. If the legitimacy of the user's identity is not properly identified and verified, it will lead to If the user's identity legitimacy is not properly identified and verified, malicious users can impersonate high authority accounts to perform illegal operations.

The system architecture proposed in this study can be used to prevent the attack techniques used by malicious users, including theft or loss of smart cards and malicious use of data, and so on. In addition, this research framework can be applied to the identity verification mechanism of smart card in multi-server environment, so in addition to the existing services, the organization still retains the ability to integrate various services into the smart. In addition, this research framework can be applied to the smart card identity verification mechanism in multi-server environment.

5.2 Future Direction

In the future, a two-step or multi-step authentication process could be incorporated in the front-end of the system's identity authentication phase to improve its elasticity, thus allowing the system to adapt to continuously evolving hacking techniques and hardware specifications. In addition, the operational procedures of our system could be implemented, so that the viability and effectiveness of our proposed system can be validated and analyzed through actual encryption and decryption operations.

References

Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., & Chang, V. (2018). A lightweight authentication protocol for IoT-enabled devices in distributed cloud computing environment. *Future Generation Computer Systems*, *78*(3), 1005-1019.

Chuang, M. C., & Chen, M. C. (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Systems with Applications*, *41*(4), 1411-1418.

Datta, P., Bhowmik, A., Shome, A., & Biswas, M. (2020). A secured smart national identity card management design using blockchain. *In Proceedings of the 2020 2nd IEEE International Conference on Advanced Information and Communication Technology (ICAICT)* (pp. 291-296). IEEE.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469-472.

Huang, M. S., & Li, H. L. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, *46*(1), 28-30.

Hsiang, H. C., & Shih, W. K. (2009). Improvement of the secure dynamic ID-based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, *31*(6), 1118-1123.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283-294.

Jangirala, S., Mukhopadhyay, S., & Das, A. K. (2017). A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards. *Wireless Personal Communications*, *95*(3), 2735-2767.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770-772.

Liao, Y. P., & Wang, S. S. (2009). A secure dynamic ID-based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, *31*(6), 24-29.

Lee, C. C., Lin, T. H., & Chang, R. X. (2011). A secure dynamic ID-based remote user authentication scheme for multi-server environment using smart cards. *Expert Systems with Applications*, *38*(1), 13863-13870.

Li, X., Xiong, Y., Ma, J., & Wang, W. (2012). An efficient and secure dynamic identity-based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Applications*, *35*(2), 763-769.

Lo, K. L. (2014). *A study of the user authentication and secret communication mechanism of websites*. Master's thesis. National Defense University, Taipei, Taiwan.

Menezes, A. J., Katz, J., Oorschot, P. V., & Vanstone, S. A. (2001). *Handbook of applied cryptography*. Boca Raton, FL: CRC Press.

Wichers, D., & Williams, J. (2017). *OWASP top 10–2017: The ten most critical web application security risks*. OWASP Foundation.

Ranganathan, C., & Ganapathy, S. (2002). Key dimensions of business-to-business web sites. *Information & Management*, *35*(6), 457-465.

Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. *ACM Computing Surveys*, 35(3), 309-329.

Sood, S. K., Sarje, A. K., & Singh, K. (2011). A secure dynamic identity-based authentication protocol for multi-server architecture. *Journal of Network and Computer Applications*, (2), 609-618.

Shunmuganathan, S., Saravanan, R. D., & Palanichamy, Y. (2015). Secure and efficient smart-card-based remote user authentication scheme for multi-server environment. *Canadian Journal of Electrical and Computer Engineering*, *38*(1), 20-30.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, *44*, 100467.

Xue, K., Hong, P., & Ma, C. (2014). A lightweight dynamic pseudonym identity-based authentication and key agreement protocol without verification tables for multi-server architecture. *Journal of Computer and System Sciences*, *80*(1), 195-206.

Yu, M., Yao, H., Qin, C., & Zhang, X. P. (2022). A comprehensive analysis method for reversible data hiding in stream-cipher-encrypted images. *IEEE Transactions on Circuits and Systems for Video Technology*, *32*(10), 7241-7254.