Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8850083, 12 pages
https://doi.org/10.1155/2020/8850083

Research Article

An Efficient Anonymous Authentication Scheme for Mobile Pay-TV Systems

Yuting Li,[1,2] Qingfeng Cheng,[1,2] and Jinzheng Cao[1,2]

[1]*Strategic Support Force Information Engineering University, Zhengzhou 450001, China*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*

Correspondence should be addressed to Qingfeng Cheng; qingfengc2008@sina.com

Received 22 April 2020; Revised 13 August 2020; Accepted 25 August 2020; Published 10 September 2020

Academic Editor: Ding Wang

Copyright © 2020 Yuting Li et al. 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.

As a component of mobile communication, the pay-TV system has attracted a lot of attention. By using mobile devices, users interact with the head end system in service providers to acquire TV services. With the growth of mobile users, how to protect the privacy of users while improving efficiency of the network has become an issue worthy of attention. Anonymous authentication schemes for mobile pay-TV systems came into being. In this paper, we analyze the shortcomings of the existing authentication protocol and then propose an improved one, which is secure against stored set attack and user traceability attack. The proposed scheme is proved to be secure. Moreover, our new scheme performs better in efficiency and storage, compared with several other schemes.

1. Introduction

With the rapid development of wireless communication technology, pay-TV systems have attracted a lot of attention as a component of mobile communication. According to Ref. [1], the number of users who used the pay-TV system reached 3.45 million in 1994, in England. Four years later, that number has doubled. TV service is developing from socialization to personalization, which means that users are able to watch their favourite TV programs anytime, anywhere. The pay-TV systems can meet the personalized needs of users. These changes have prompted the emergence of many communication systems for mobile TV services [2, 3].

In a pay-TV system, there are two entities, a service provider and a user. When a user needs a TV service, she interacts with the head end system (HES) of the service provider. The pay-TV system generally uses a conditional access system (CAS) to handle interactions between end users and service providers. Figure 1 shows the main components of CAS, which controls the reception of TV services by encrypting transmission services to ensure that only authorized users can access certain services. The transmitter (TX) and the receiving module (RX) are subsystems responsible for signal transmission and reception, respectively. The multiplexer (MUX) is responsible for multiplexing audio and video into the MPEG-2 transport stream, while the demultiplexer (DEMUX) is responsible for separating audio and video from the MPEG-2 transport stream. The subscriber authorization system (SAS) and subscriber management system (SMS) authorize and manage users separately.

Encryption and authentication play significant roles in CAS for mobile pay-TV systems. Obviously, we can see encryption and authentication processes Figure 1. The encryptor and the decryptor are responsible for encryption. When a user needs to obtain a service, she sends subscription and authentication messages to HES. In detail, the encryption keys must be distributed to all subscribers so that they can receive and decrypt the broadcasts they are entitled to under the terms of their subscriptions. Each receiver first filters the corresponding EMM messages and decrypts the SK and then decrypts ECM using SK. After the authorized user gets CW from ECM, she could descramble the content.

As for highly distributed mobile TV service delivery architectures [4], cloud computing models are unable to meet

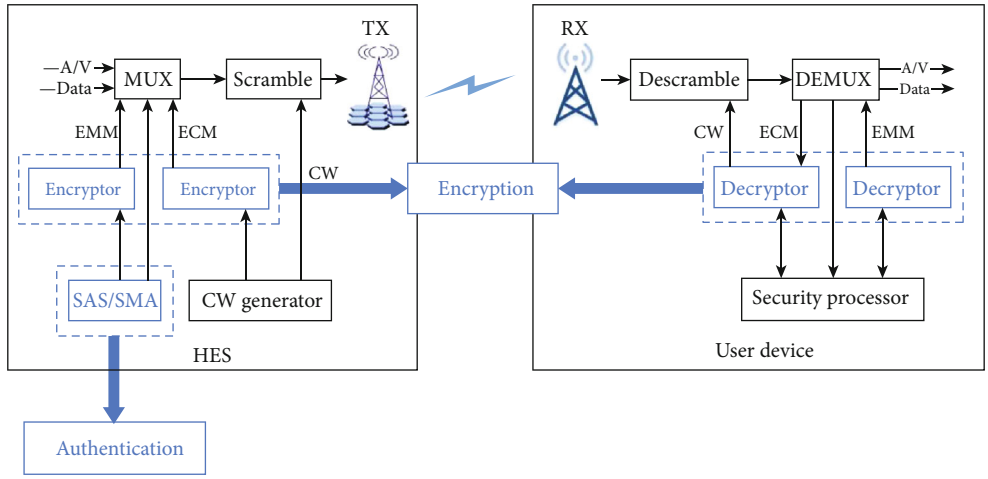

Figure 1: Encryption and authentication in conditional access system. Encryption and authentication process are marked in blue.

demands. The massive data generated by various access devices has made cloud network bandwidth even more limited, causing greater data bottlenecks [5]. For example, delay-sensitive business systems do not work well in cloud computing. These delay-sensitive services are often located at the edge of the data centers and can use nearby computing resources to complete calculations or reduce delays.

On the other hand, data generated by the terminal TV devices usually involves personal privacy information. Uploading these data to the cloud data center not only consumes a lot of bandwidth resources but also increases the risk of user privacy leakage [6, 7]. In order to deal with this problem, the user's identity and password are involved in anonymous authentication protocols. The role of user-generated passwords is becoming more prominent in wireless mobile networks [8]. Two-factor anonymous authentication schemes have been proposed to wireless networks for a long time [9, 10]. Moreover, three-factor authentication and key agreements have also been widely used for cloud environment [11, 12]. Besides, fuzzy commitment with low latency can also be employed to ensure high efficiency [13].

In recent years, mobile pay-TV systems have risen in popularity due to their extensive application. The most challenging issue is providing secure authentication [14]. There have been many studies on anonymous authentication schemes used for HES. In Ref. [15], Far and Alagheband designed a lightweight anonymous authentication protocol. We found that this protocol is suffering from the risk of revealing user's password. Besides, there is still room for improvement in storage. The main contributions of our paper are listed below:

(i) We reveal Far and Alagheband's protocol is suffering from the risk of revealing user's privacy. Besides, there is still room for improvement in storage

(ii) We propose a new efficient anonymous authentication scheme based on Far and Alagheband's protocol

(iii) The proposed anonymous authentication scheme in the paper performs better in computing efficiency and storage, which is more suitable for resource-constrained devices in edge computing environment

The rest of the paper is planned as follows. In Section 2, we describe related authentication schemes used in pay-TV systems. In Section 3, the preliminaries needed in protocol design are listed. The proposed anonymous authentication scheme is described in detail in Section 4. In Section 5, we give analysis of security proof and security features. Performance comparison is shown in Section 6. The conclusion is given in Section 7.

2. Related Work

In this section, we first introduce secure CASs and categorize pay-TV systems in three groups. Encryption-based pay-TV systems are the most classic category. Signature-based pay-TV systems are the most practical application. Authentication schemes for pay-TV systems are the most important point of our attention. Table 1 shows the relationships of some related works in chronological order.

2.1. Secure CASs. In 1992, ITU first proposed the standards for CASs in pay-TV systems [16]. However, this standard does not provide authentication capabilities for service providers. Since then, in order to further strengthen security, the academic community has proposed some CASs based on symmetric cryptography. In this type of CASs, users must share group keys used to encrypt and decrypt.

Zhu proposed a one-to-many CAS [17]. This system adopted the word-counting model for the first time, which improved the overall efficiency of the system to some extent. However, because the number of keys that a user needs to save was directly proportional to the number of related users, the storage and distribution of keys became very complicated, so this type of CASs was not suitable for practical applications. In general, CASs based on symmetric encryption could not avoid complicated key distribution problems. At the same time, such systems could not provide nonrepudiation.

Table 1: The relationship of related works.

Schemes	Year	Base article	Contribution
Song and Korba [29]	2003	Lee et al. [28]	Designed an improved version using RSA blind signature technology
Wang and Laith [21]	2008	Huang et al. [20]	Proposed an improved key distribution scheme
Sun and Leu [34]	2009	Yang and Chang [31]	Designed the first one-to-many authentication scheme
Wang and Qin [35]	2012	Sun and Leu [34]	Presented an enhanced scheme against impersonation attacks
Kim and Lee [33]	2012	Chen et al. [32]	Gave an improved version against password guessing attack and impersonation attack
Arshad et al. [36]	2017	Wang and Qin [35]	Designed an authentication scheme without bilinear pairings
Far and Alagheband [15]	2018	Chen et al. [32]	Proposed a strengthened scheme to alleviate its security risks

In 2019, Pal and Alam proposed a channel package free centralized key distribution scheme, which was based on dynamicity of the groups [18]. The scheme used finite state machine (FSM) and optimal binary search tree (OBST) data, providing leaving and joining mechanisms for both batch users and single user. Recently, Kumar et al. [19] designed a key management protocol for access control for the pay-TV system, using the theory of numbers. The protocol is said to achieve the minimum communication complexity and storage overhead.

2.2. Encryption-Based Pay-TV Systems. In 2004, Huang et al. divided users into different groups according to their various preferences, and each group shared the key [20]. However, Wang and Laith found that Huang et al.'s protocol was vulnerable to key leakage attack [21]. To enhance security, they proposed an improved key distribution scheme. In the same year, Sun et al. introduced a four-layer key hierarchy model, supporting more users to make flexible choices [22]. These CASs have a common feature in that one request message corresponds to one reply request, so they cannot respond to multiple requests in a short time. The one-to-many CASs, which can respond to many service requests at the same time, have become a new research direction.

In 2005, Yeung et al. constructed a new CAS based on the RSA algorithm. In their protocol, the media service provider and the proxy service provider needed to jointly encrypt the TV programs [23]. Several years later, Yeu and Huang presented an attribute-based encryption-based access control scheme and extended it with a revocation mechanism [24]. However, the scheme was pointed to be vulnerable to collusion attacks by Rial [25].

2.3. Signature-Based Pay-TV Systems. As one of the cryptographic primitives, signature provides the integrity and authentication of messages [26, 27]. To solve this kind of problem, Lee et al. proposed an authentication protocol based on digital signature technology [28]. However, this protocol could not provide anonymity for service providers. To strengthen its security, Song and Korba designed an improved version of the authentication protocol, using RSA blind signature technology [29]. Since then, Roh and Jung also adopted RSA-based proxy signature technology and designed a new authentication scheme [30]. However, the communication cost of their scheme was relatively high and it was not suitable for practical application.

2.4. Authentication Schemes for Pay-TV Systems. The authentication scheme applicable to pay-TV systems cannot be directly applied to mobile pay-TV systems. Yang and Chang designed an authentication scheme for mobile pay-TV systems using elliptic curve cryptography [31]. However, Chen et al. [32] pointed out that there were security issues in Yang and Chang's scheme and proposed an anonymous authentication protocol to solve the insecure risks. They claimed that their protocol is better for applications with low power-consuming devices and high security requirements. However, Kim and Lee showed that Chen et al.'s protocol suffers the risks in password guessing attack and impersonation attack and gave an improved version [33]. In 2018, Far and Alagheband also enhanced the security in Chen et al.'s protocol to alleviate its security risks [15].

To improve the performance, Sun and Leu designed the first one-to-many authentication scheme in 2009 [34]. The scheme also used elliptic curve cryptography, suitable for access control in mobile pay-TV systems. However, Wang and Qin found that Sun and Leu's scheme had security risks [35]. The adversary could not only pretend to be a mobile set (MS) to deceive HES but also pretend to be MS to deceive HES. Moreover, Sun and Leu's scheme could not prevent unauthorized entities from accessing mobile TV programs. In order to strengthen security, Wang and Qin proposed a strengthened authentication protocol and claimed that their protocol could resist various common attacks. Based on Wang and Qin's scheme [34], Arshad et al. designed an encryption-based authentication scheme for mobile pay-TV. This scheme did not use bilinear pairings and was easily implemented on FPGA boards [36].

In 2013, Liu and Zhang designed an identity-based encryption scheme based on bilinear pairings [37]. In addition, the batch verification technique allowed the service provider to authenticate various requests from different subscribers.

Sabzinejad et al.'s scheme was also designed using a bilinear pair in 2016 [38]. Its running time was shorter than previous solutions, but it was not suitable for lightweight devices. Kuo proposed an authentication scheme based on smart cards and biometrics for mobile pay-TV, which could be used on lightweight smart card devices for multiserver environments [39]. Wu et al. proposed an authentication scheme based on user signatures for mobile pay-TV, but this scheme could not guarantee user anonymity [40]. Zhu presented a deniable authentication protocol for pay-TV system based on chaotic maps, which is called DAP-TV [41]. In 2020,

Table 2: Notations of entities and parameters.

Entities	Description	Parameters	Description
HES	Head end system	S	The server
MS	Mobile set	U	The user
SAS	Subscriber authorization system	ID	Identity of the user
SMS	Subscriber management system	PW	Password of the user
CW	Control word	b	Random number
CAS	Conditional access system	T	Timestamp
ECM	Entitlement control message	ΔT	Specified maximum time difference
EMM	Entitlement management message	N	User registeration number
DBS	Data base server	Θ	Token for issue phase
MUX	Multiplexer	γ	Token for subscription phase
DEMUX	Demultiplexer	η	Token for hand-off phase
TX	Transmitter	$h(\ )$	One-way hash function
RX	Receiving module	x	Secret key of DBS
DVB	Digital video broadcast	$\mathscr{A}$	The adversary

Kumaravelu et al. [14] designed an anonymous scheme which can authenticate both users and HES, with low computational cost.

3. System Model and Security Requirements

In this section, the operating mechanism of mobile pay-TV systems is explained at first. The security features required in anonymous authentication schemes and adversary capabilities are then briefly explained.

3.1. Anonymous Authentication Model for Mobile Pay-TV Systems. Table 2 shows notations of entities and parameters. The mobile pay-TV system consists of two important components, the head end system (HES) and the mobile set (MS). HES not only has powerful service content processing capabilities but also contains SAS/SMS. SAS/SMS is mainly responsible for authentication and key management, payment management, and subscription information management. MS is a user equipment that can use the mobile Internet connection to HES to obtain TV services.

In general, when a user wants to purchase a mobile pay-TV service, she needs to register the private information in HES, such as an ID number and email address. When the user needs TV services, his MS will send a request message for MS authentication and a service content request to HES. If the MS passes the HES authentication, the HES will broadcast a request message for the HES authentication to all nearby mobile sets. After the MS completes the authentication of the HES, the user can obtain service rights and enjoy the mobile pay-TV service. When the user wants to switch to another TV service, the MS and HES need to conduct mutual authentication again.

More specifically, there are four steps in the process of mobile TV and HES authentication and subscription services. In the initialization phase, DBS is responsible for generating system parameters and secret parameters required by MS. All HESs can obtain the parameters stored in DBS, which are generated in the initialization phase. In the issue phase, MS sends a log-in request to one HES to obtain a service then authenticates with this HES. As a result, the HES will issue a token for MS, which will be used in the subscription phase to subscribe a service. When the mobile TV wants to move to another area covered by other HES, all the MS needs to do is to authenticate with the new HES, not to reregister or send a log-in request. These four steps are shown in Figure 2.

3.2. Security Requirements. The anonymous authentication protocols used in mobile pay-TV systems need to provide mutual authentication, forward security, and privacy protection of each entity. In addition, the importance of user anonymity and user untraceability is more emphasized in mobile pay-TV systems.

3.2.1. Mutual Authentication. HES and MS need to perform mutual authentication, to conduct subsequent key management, payment management, and subscription management. For resource-constrained devices, the efficiency of authentication should be taken into consideration.

3.2.2. Forward Security. One of the characteristics of mobile users is frequent log-in and log-out. Therefore, when a mobile user leaves a communication network, others cannot infer any user information from the encrypted message left by the user. Forward security means that the authenticated keys generated from each session are independent of each other.

3.2.3. User Anonymity. User anonymity is the most basic requirement in an anonymous authentication protocol, which hides the user's identity and communication relationship in the communication process through a certain method. This usually means that the user's identity cannot be obtained by anyone, whether he is an internal attacker or an external attacker. In other words, the identity of the user cannot be publicly transmitted in plaintext.

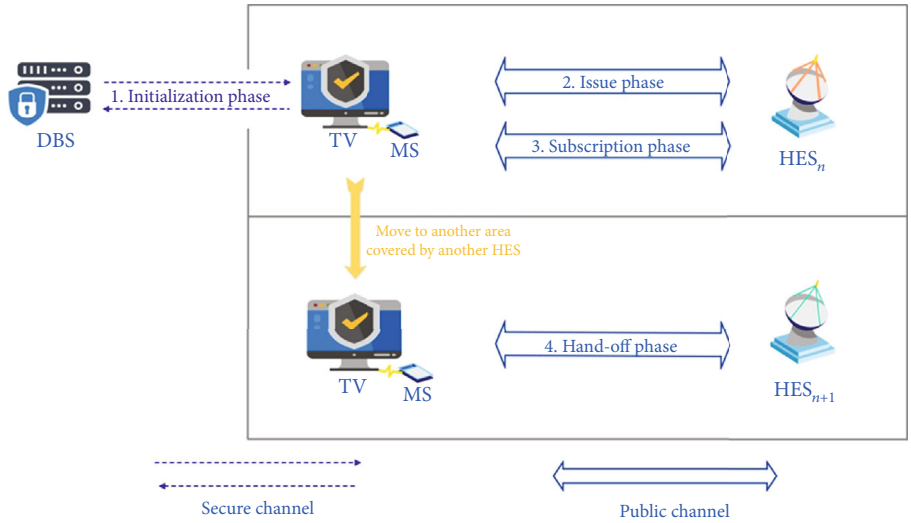

Figure 2: Anonymous authentication model for mobile pay-TV system. The initialization phase is performed on secure channel, while the other three phases can be performed on public channel.

3.2.4. User Untraceability. User untraceability has many implications. Malicious attackers or other users cannot determine which servers a user has logged in to or how many times a user has logged in to a server. Untraceability can ensure that even if the user reveals his identity at a certain stage, it will not help the adversary to identify the user at other stages. An effective way to achieve untraceability is to randomize the information transmitted in each step of the authentication phase.

3.2.5. Privacy Protection. Privacy protection means that the information of both MS and HES should be unavailable to others. In mobile pay-TV systems, the user logs in anonymously and does not want anyone to know her identity information. This requires that the identity information cannot be stored and transmitted in plain text.

3.3. Adversary Capabilities. As defined in other anonymous authentication protocols for mobile pay-TV systems, adversaries have the ability to do all passive attacks, such as eavesdropping on messages in public channel. Moreover, the adversary is allowed to obtain all parameters stored in DBS.

In order to prove that our scheme has more advantages in security, we have given adversaries the ability to obtain stored sets. That means the information stored in smart cards of MS and HES is not secure anymore.

The capabilities of adversaries are described briefly below:

(i) $\mathcal{A}$ can eavesdrop on messages in public channel

(ii) $\mathcal{A}$ can obtain all parameters stored in DBS

(iii) $\mathcal{A}$ can achieve all information stored in stored set of MS

(iv) $\mathcal{A}$ can be a internal attacker

4. The Proposed Scheme

In this section, we explain an improved scheme of Far and Alagheband's scheme. Our improved scheme also has four phases as depicted in Section 3, the initialization phase, issue phase, subscription phase, and hand-off phase. The initialization phase is performed on secure channel, while the other three phases can be performed on public channel. These four phases are described, respectively, as below. The notations used in this section are shown in Table 2.

4.1. Initialization Phase. In the initialization phase, the MS should register in SAS/SMS through DBS, which stores data in HES. This phase needs to be performed on a secure channel. More details are listed as follows.

MS: chooses a random number b and generates its password PW, then computes $\mathrm{PWB} = h(\mathrm{PW}\|b)$. After that, it sends ID and PW to DBS of HESn.

DBS: after receiving ID and PW from the MS, DBS computes $Q = h(\mathrm{ID}\|x) \oplus \mathrm{PWB}$, $R = h(\mathrm{PWB}\|\mathrm{ID}) \oplus h(\mathrm{ID}\|x)$, and $t = h(\mathrm{PWB}\|h(\mathrm{ID}\|x))$. Here, x is the secret key of the DBS, which is generated by HESn. Finally, DBS stores R and t, then sends Q and R to MS.

MS: after receiving Q and R from DBS, MS stores Q and R .

The initialization phase is shown in Figure 3.

4.2. Issue Phase. Before a mobile TV wants to obtain a service, the MS needs to send a service start request to HESn, that is, log-in request. After sending a log-in request, MS and HESn authenticate each other in the issue phase. As a result, HESn will issue a token for MS, which will be used in the subscription phase. The detailed authentication process is described in Figure 4.

MS: computes $\mathrm{PWB} = h(\mathrm{PW}\|b)$ and verifies $R = Q \oplus \mathrm{PWB} \oplus h(\mathrm{PWB}\|\mathrm{ID})$. If verified, it then computes $W = h(h(\mathrm{PWB}\|Q \oplus \mathrm{PWB}) \oplus T_1)$, $\mathrm{CID} = W \oplus h(W\|T_1), C = h(R\|\mathrm{CID}\|T_1)$,

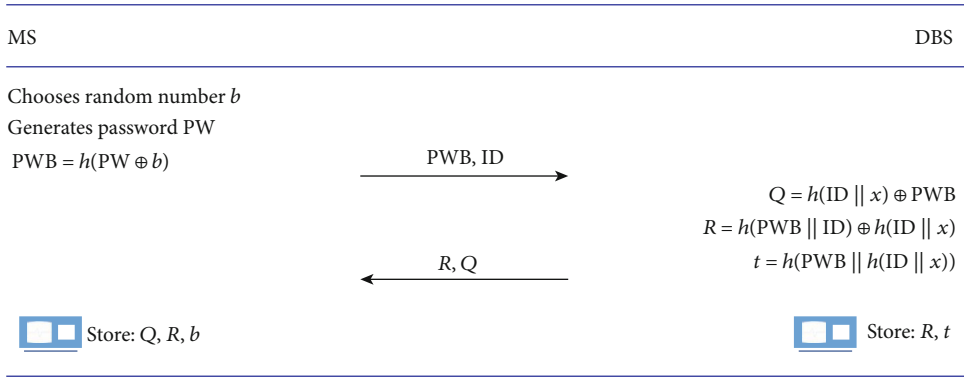

Figure 3: Initialization phase. The initialization phase needs to be performed on a secure channel.

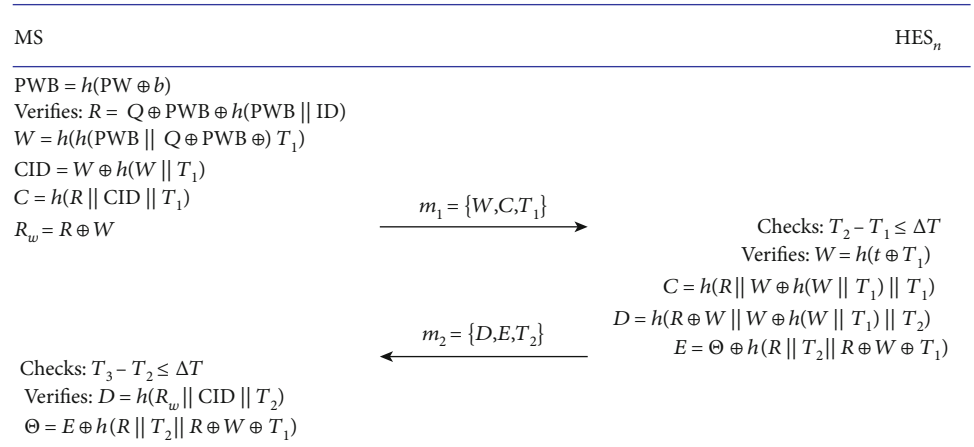

Figure 4: Issue phase. The issue phase can be performed on public channel.

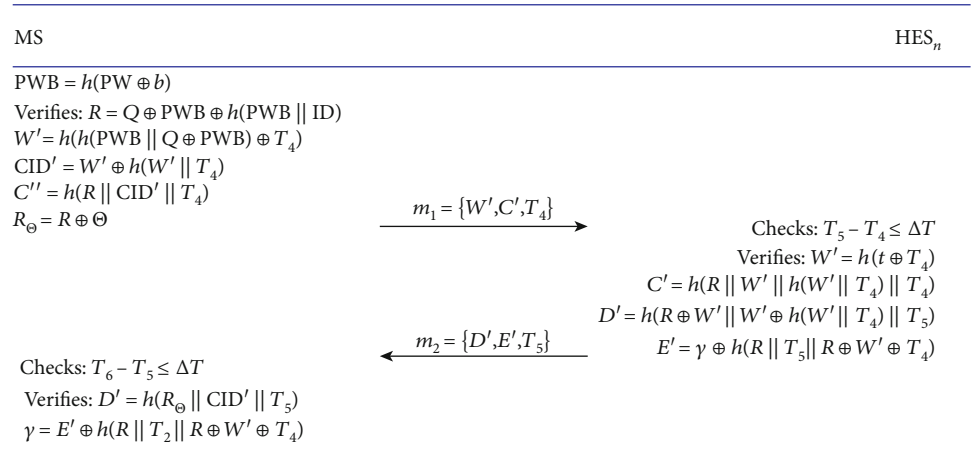

Figure 5: Subscription phase. The subscription phase can be performed on public channel.

and $R_W = R \oplus W$, and finally sends $m_1 = \{W, C, T_1\}$ to HESn at T_1.

HESn: receives message at T_2. It first checks $T_2 - T_1 \le \Delta T$, then verifies $W = h(t \oplus T_1)$ and $C = h(R \| W \oplus h(W \| T_1) \| T_1)$. Next, it chooses a token Θ and computes $D = h(R \oplus W \| W \oplus h(W \| T_1) \| T_2)$, $E = \Theta \oplus h(R \| T_2 \| R \oplus W \oplus T_1)$, and finally sends $m_2 = \{D, E, T_2\}$ to MS at T_3.

MS: after receiving m_2, it first checks $T_3 - T_2 \le \Delta T$. Then, it verifies $D' = h(R_W \| CID \| T_2)$. The authentication key is computed as $\Theta = E \oplus h(R \| T_2 \| R \oplus W \oplus T_1)$.

4.3. Subscription Phase. Once the MS has obtained the token from the HESn, it can use it to subscribe to the service. Except for the token Θ from the issue phase to participate in the

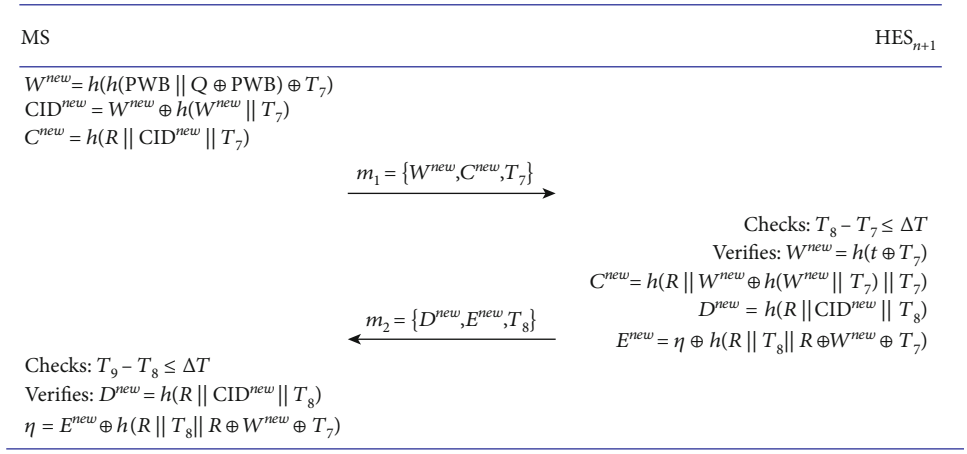

Figure 6: Hand-off phase. The hand-off phase can be performed on public channel.

operation, other steps are similar to the issue phase. The details are showed in Figure 5.

MS: computes $\text{PWB} = h(\text{PW} \| b)$ and verifies $R = Q \oplus \text{PWB} \oplus h(\text{PWB} \| \text{ID})$. If verified, it then computes $W' = h(h(\text{PWB} \| Q \oplus \text{PWB}) \oplus T_4)$, $\text{CID}' = W' \oplus h(W' \| T_4)$, $C' = h(R \| \text{CID}' \| T_4)$, and $R_\Theta = R \oplus \Theta$, and finally sends $m_1 = \{W', C', T_4\}$ to HESn at T_4.

HESn: receives message at T_5. It first checks $T_5 - T_4 \le \Delta T$, then verifies: $W' = h(t \oplus T_4)$, $C' = h(R \| W' \oplus h(W' \| T_4) \| T_4)$. Next, it chooses a new token γ and computes $D' = h(R \oplus \Theta \| W' \oplus h(W' \| T_4) \| T_5)$ and $E' = \gamma \oplus h(R \| T_5 \| R \oplus W' \oplus T_4)$ and finally sends $m_2 = \{D', E', T_5\}$ to MS at T_6.

MS: after receiving m_2, it first checks $T_6 - T_5 \le \Delta T$, then verifies $D' = h(R_\Theta \| CID' \| T_5)$. The authentication key is computed as $\gamma = E' \oplus h(R \| T_2 \| R \oplus W' \oplus T_4)$.

4.4. Hand-Off Phase. When a mobile user wants to move from the area covered by HESn to another area covered by HES$n+1$, he does not need to reregister or send a log-in request. All the MS needs to do is to authenticate with the new HES$n+1$. The details are showed in Figure 6.

MS: first computes $W^{\text{new}} = h(h(\text{PWB} \| Q \oplus \text{PWB}) \oplus T_7)$, $\text{CID}^{\text{new}} = W^{\text{new}} \oplus h(W^{\text{new}} \| T_7)$, and $C^{\text{new}} = h(R \| \text{CID}^{\text{new}} \| T_7)$, and then sends $m_1 = \{W^{\text{new}}, C^{\text{new}}, T_7\}$ to HES$n+1$ at T_7.

HES$n+1$: receives message at T_8. It first checks $T_8 - T_7 \le \Delta T$, then verifies $W^{\text{new}} = h(t \oplus T_7)$ and $C^{\text{new}} = h(R \| W^{\text{new}} \oplus h(W^{\text{new}} T_7) \| T_7)$. Next, it chooses a new token η and computes $D^{\text{new}} = h(R \| \text{CID}^{\text{new}} \| T_8)$, $E^{\text{new}} = \eta \oplus h(R \| T_8 \| W^{\text{new}} \oplus R \oplus T_7)$. Finally, it sends $m_2 = \{D^{\text{new}}, E^{\text{new}}, T_8\}$ to MS at T_9.

MS: after receiving m_2, it first checks $T_9 - T_8 \le \Delta T$, then verifies $D^{\text{new}} = h(R \| \text{CID}^{\text{new}} \| T_8)$. The authentication key to get services for new HES is set as $\eta = E^{\text{new}} \oplus h(R \| T_8 \| R \oplus W^{\text{new}} \oplus T_7)$.

5. Security Analysis

Security analysis is composed of two subsections. First, we prove our improved scheme to be secure using the formal method in Section 5.1. Then, the main security features in our scheme are shown in Section 5.2.

5.1. Formal Security Analysis. In this subsection, we will show that our improved scheme can resist eavesdropping attack, stored set attack, and internal attack. The approaches proposed in literature [15, 42, 43] are employed in this part. The adversary capabilities are given in Section 3.

First, we give the definition that the adversary successfully breaks the scheme [42]. The first thing is to explain notations:

(i) Experiment function (EXP): $\mathcal{A}$ successfully obtains the required information

(ii) Success function (Succ): $\mathcal{A}$'s probability of success in obtaining the key secret information

Definition 1. If the probability of success is negligible, the scheme is secure against assumed $\mathcal{A}$.

$$\text{Succ} = \Pr\left[\text{EXP}^{\text{function}}\right] \le \varepsilon. \tag{1}$$

Theorem 2. *The adversary $\mathcal{A}$ eavesdrop on messages in public channel. $\mathcal{A}$ can break the scheme with probability* $\Pr[EXP^{hash}] \le \varepsilon$, *where ε is negligible.*

Proof of Theorem 1. $\mathcal{A}$ can eavesdrop $m_1 = \{W, C, T_1\}$ in public channel. We describe the subsequent actions of $\mathcal{A}$ in Algorithm 1, which consists of set up, challenge, and guess.

It is obviously to see that $\mathcal{A}$ must correctly guess the value of $\text{ID}, x, \text{PW}, b$ to pass the algorithm. The probability of correctly guessing these four values is less than $(1/2)^{\text{length}}$:

$$\text{Succ}_{\text{ID}} = \Pr\left[\text{EXP}^{h\text{ash}-\text{ID}}\right] \le \left(\frac{1}{2}\right)^{\text{ID}-\text{length}}, \tag{2}$$

$$\text{Succ}_x = \Pr\left[\text{EXP}^{\text{hash}-x}\right] \le \left(\frac{1}{2}\right)^{x-\text{length}}, \tag{3}$$

Set up: Input $\{W, C, T_1\}$ eavesdropped from public channel. If success, output 1. Otherwise, output 0.
Challenge:
(i) Eavesdrop $\{W, C, T_1\}$ from public channel
(ii) Compute $W = h(t \oplus T_1)$. Here $t = h(PWB \| h(ID \| x))$, $PWB = h(PW \| b)$.
(iii) Choose randomly ID^*, x^*, PW^*, b^* as the value of ID, x, PW, b
(iv) Compute $h(h(h(PW^* \| b^*) \| h(ID^* \| x^*)) \oplus T_1 = W^*$
Guess: If $W^* = W$, accept the value of ID^*, x^*, PW^*, b^*. Return 1. Otherwise, return 0.

Algorithm 1

Set up: Input R, b corrupted from MS. If success, output 1. Otherwise, output 0.
Challenge:
(i) Corrupt R, b
(ii) Choose randomly PW^*, ID^*, x^* as the value of user's password, identity and server's secret key
(iii) Compute $R^* = h(h(PW^* \| b) \| ID^*) \oplus h(ID^* \| x^*)$.
Guess: If $R^* = R$, accepts the value of PW^*, ID^*, x^*. Return 1. Otherwise, returns 0.

Algorithm 2

Set up: Input Q, b corrupted from MS. If success, output 1. Otherwise, output 0.
Challenge:
(i) Corrupt Q, b
(ii) Choose randomly PW^*, ID^*, x^* as the value of user's password, identity, and server's secret key
(iii) Compute $Q^* = h(ID^* \oplus x^*) \oplus h(PW^* \| b)$
Guess: If $Q^* = Q$, accepts the value of PW^*, ID^*, x^*. Return 1. Otherwise, returns 0.

Algorithm 3

$$\text{Succ}_{PW} = \Pr\left[\text{EXP}^{\text{hash}-PW}\right] \leq \left(\frac{1}{2}\right)^{PW-\text{length}}, \quad (4)$$

$$\text{Succ}_{b} = \Pr\left[\text{EXP}^{\text{hash}-b}\right] \leq \left(\frac{1}{2}\right)^{b-\text{length}}. \quad (5)$$

Thus, $\mathcal{A}$ an break the scheme with probability: $\Pr[\text{EXP}^{hash}] \leq (1/2)^{(ID \| x \| PW \| b)-\text{length}} \leq \varepsilon$, where ε is negligible.

Theorem 3. *The adversary $\mathcal{A}$ can achieve the stored set of MS. $\mathcal{A}$ can break the scheme with probability* $\Pr[EXP^{hash}] \leq \varepsilon$, *where ε is negligible.*

Proof of Theorem 3. $\mathcal{A}$ can achieve the stored set of MS. We describe the subsequent actions of $\mathcal{A}$ in Algorithm 2 and Algorithm 3, which represents the situation when $\mathcal{A}$ obtains R, b and Q, b, respectively.

The key to successfully passing Algorithm 2 is to correctly guess the value of PW^*, ID^*, x^*. The probability of correctly guessing these four values is less than $(1/2)^{\text{length}}$:

$$\text{Succ}_{PW} = \Pr\left[\text{EXP}^{\text{hash}-PW}\right] \leq \left(\frac{1}{2}\right)^{PW-\text{length}}, \quad (6)$$

$$\text{Succ}_{ID} = \Pr\left[\text{EXP}^{\text{hash}-ID}\right] \leq \left(\frac{1}{2}\right)^{ID-\text{length}}, \quad (7)$$

$$\text{Succ}_{x} = \Pr\left[\text{EXP}^{\text{hash}-x}\right] \leq \left(\frac{1}{2}\right)^{x-\text{length}}. \quad (8)$$

Thus, $\mathcal{A}$ can break the scheme with probability: $\Pr[\text{EXP}^{\text{hash}}] \leq (1/2)^{(PW \| ID \| x)-\text{length}} \leq \varepsilon$, where ε is negligible.

The key to successfully passing Algorithm 3 is to correctly guess the value of PW^*, ID^*, x^*. The probability of correctly guessing these four values is less than $(1/2)^{\text{length}}$:

$$\text{Succ}_{PW} = \Pr\left[\text{EXP}^{\text{hash}-PW}\right] \leq \left(\frac{1}{2}\right)^{PW-\text{length}}, \quad (9)$$

$$\text{Succ}_{ID} = \Pr\left[\text{EXP}^{\text{hash}-ID}\right] \leq \left(\frac{1}{2}\right)^{ID-\text{length}}, \quad (10)$$

$$\text{Succ}_{x} = \Pr\left[\text{EXP}^{\text{hash}-x}\right] \leq \left(\frac{1}{2}\right)^{x-\text{length}}. \quad (11)$$

Thus, $\mathcal{A}$ can break the scheme with probability: $\Pr[\text{EXP}^{\text{hash}}] \leq (1/2)^{(PW \| ID \| x)-\text{length}} \leq \varepsilon$, where ε is negligible.

Theorem 4. *The adversary $\mathcal{A}$ be an internal attacker. $\mathcal{A}$ can break the scheme with probability* $\Pr[EXP^{hash}] \leq \varepsilon$, *where ε is negligible.*

Set up: Input $\{W, C, T_1\}$ eavesdropped from public channel. If success, output 1. Otherwise, output 0.
Challenge:
(i) Receive $\{W, C, T_1\}$ from public channel
(ii) Searches R and t, where $t = h(\mathrm{PWB}\|h(ID\|x))$
(iii) Choose randomly $\mathrm{PW}^*, \mathrm{ID}^*, b^*, x^*$
(iv) Compute $R^* = h(h(\mathrm{PW}^*\|b^*)\|\mathrm{ID}^*\|h(\mathrm{ID}^*\|x^*)$, $t^* = h(h(\mathrm{PW}^*\|b^*)\|h(\mathrm{ID}^*\|x^*)$
Guess: If $R^* = R$ or $t^* = t$, accepts the value of ID^*, b^*. Return 1. Otherwise, returns 0.

Algorithm 4

Proof of Theorem 4. $\mathscr{A}$ can be a malicious server, as an internal attacker. Even so, $\mathscr{A}$ has no way of knowing identity of the user. We describe the subsequent behavior of $\mathscr{A}$ in Algorithm 4.

Since the hash functions we use are one-way secure, if $\mathscr{A}$ wants to know the value of ID, b to pass the algorithm, they can only guess. The probability of correctly guessing these two values is less than $(1/2)^{\mathrm{length}}$:

$$\mathrm{Succ}_{\mathrm{PW}} = \Pr\left[\mathrm{EXP}^{\mathrm{hash-PW}}\right] \leq \left(\frac{1}{2}\right)^{\mathrm{PW-length}}, \quad (12)$$

$$\mathrm{Succ}_{\mathrm{ID}} = \Pr\left[\mathrm{EXP}^{\mathrm{hash-ID}}\right] \leq \left(\frac{1}{2}\right)^{ID-\mathrm{length}}, \quad (13)$$

$$\mathrm{Succ}_{b} = \Pr\left[\mathrm{EXP}^{\mathrm{hash}-b}\right] \leq \left(\frac{1}{2}\right)^{b-\mathrm{length}}, \quad (14)$$

$$\mathrm{Succ}_{x} = \Pr\left[\mathrm{EXP}^{\mathrm{hash}-x}\right] \leq \left(\frac{1}{2}\right)^{x-\mathrm{length}}. \quad (15)$$

Therefore, $\mathscr{A}$ can break the scheme with probability: $\Pr[\mathrm{EXP}^{\mathrm{hash}}] \leq (1/2)^{(\mathrm{ID}\|b)-\mathrm{length}} \leq \varepsilon$, where ε is negligible.

In summary, our improved scheme can resist eavesdropping attack, stored set attack, and internal attack.

5.2. Security Features. In this subsection, we first explain the main changes in our improved scheme compared with Far and Alagheband's scheme.

(i) Bind x to R and Q

In the initialization phase of Far and Alagheband's protocol, R and Q are stored directly in DBS. The user's identity is hidden in R and Q so that the user does not need to reveal its identity when logging in and out. However, there are security risks in storing R, Q, and $Q \oplus \mathrm{PWB}$ in the DBS. As long as the adversary reveals DBS, she can obtain PWB by exclusive OR. This not only brings the leakage of user identity but also causes the risk of user untraceability. In our new scheme, we add the server's secret key x and make slight changes when calculating R and Q. Thus, the adversary can no longer recover user's privacy information through data in DBS.

(ii) Remove the random numbers n in the issue phase and subscription phase

Table 3: Notations of entities and parameters.

Security features	Far and Alagheband's scheme	The improved scheme
Mutual authentication	Yes	Yes
Forward secrecy	Yes	Yes
User anonymity	Yes	Yes
User untraceability	No	Yes
Privacy protection	No	Yes
Stored set attack	No	Yes

Table 4: Comparison of operation numbers in each scheme.

Schemes	A	B	C	D	E	F	G	H
The scheme in [32]	6	0.78	7	0.91	7	0.91	4	5
The scheme in [33]	7	0.91	20	1.3	7	0.91	4	5
The scheme in [15]	3	0.39	6	0.78	4	0.52	3	4
Our scheme	3	0.39	6	0.78	4	0.52	3	3

Note: *A*: the number of hash operations in the initialization phase. *B*: the execution time of the initialization phase (μs). *C*: the number of hash operations by user side in the issue phase. *D*: the execution time by user side of the issue phase (μs). *E*: the number of hash operations by server side in the issue phase. *F*: the execution time by server side of the issue phase (μs). *G*: the number of parameters in the stored set. *H*: the number of parameters transmitted on public channel.

The introduction of random numbers is to ensure that the authentication keys generated by each session are independent of each other, in order to meet the forward security of the anonymous authentication protocol. In Far and Alagheband's protocol, the random numbers n is used. Actually, each time a session generates an authentication key, a time stamp is required. Here, the time stamp $T_i (i = 1, \cdots, 6)$ not only provides the function of mutual authentication, but also introduces freshness. Therefore, our scheme can still guarantee forward security without using random numbers.

As a result of the changes, the security of the new scheme has been improved in terms of user untraceability and privacy protection. Table 3 shows the comparison of our improved scheme and Far and Alagheband's scheme.

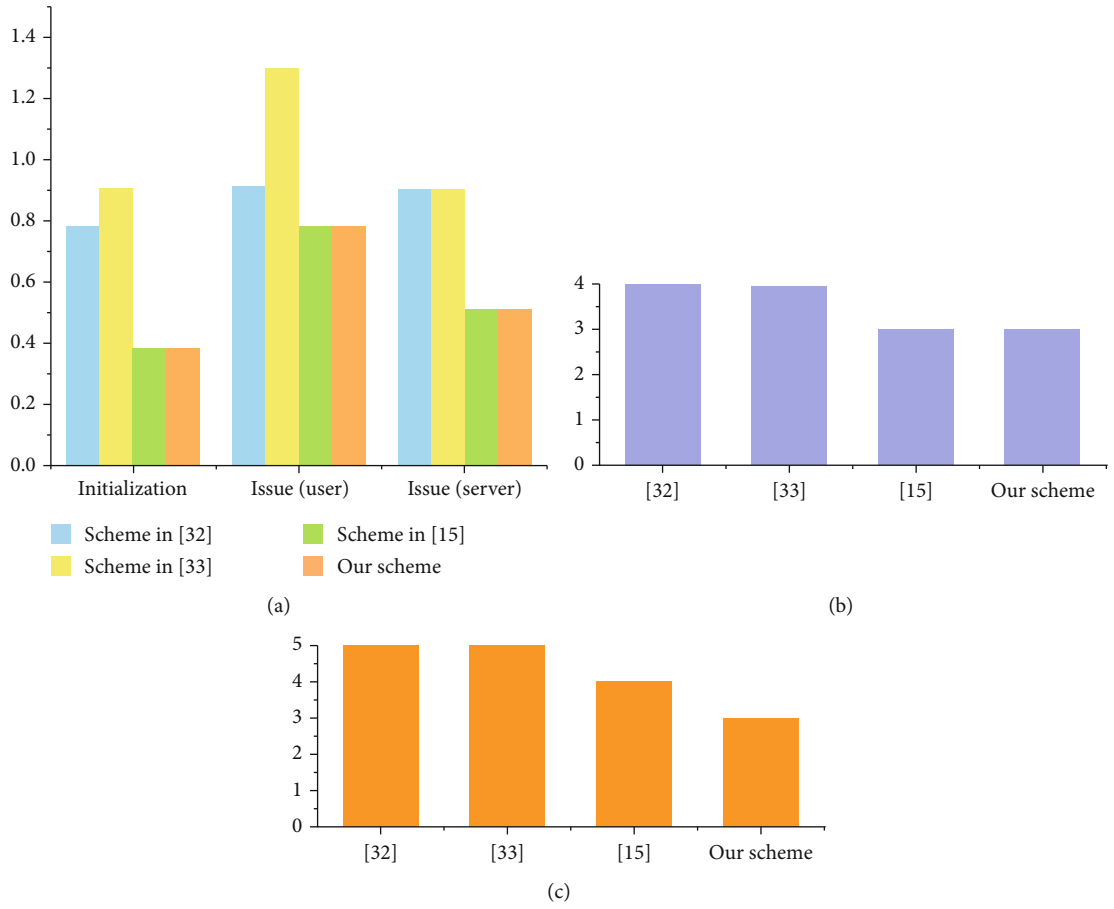

Figure 7: Comparison of execution time and parameter numbers. (a) Comparison of execution time. (b) Comparison of parameters in the stored set. (c) Comparison of parameters transmitted on public channel.

5.2.1. Mutual Authentication. In each session, HES and MS must first perform mutual authentication, using the preassigned R, Q, and t. We bind the server's secret key x and the user's identity ID when calculating R, Q, and t, to ensure the confidentiality of them. The one-way hash function also provides an efficient method for mutual authentication.

5.2.2. Forward Security. Forward security means that the authenticated keys generated from each session are independent of each other. In our new scheme, the time stamps T_i $(i = 1, \cdots, 6)$ introduce the freshness of each session. Different $T_i (i = 1, \cdots, 6)$ participating in the operation will generate different authentication keys.

5.2.3. User Anonymity. User anonymity means that the user's identity ID cannot be obtained by internal attackers or external attackers. In our new scheme, the identity ID of the user is not be publicly transmitted in plaintext, while it is placed in a hash function. Moreover, the server has no access to recover the user's identity ID from R and t stored in DBS.

5.2.4. User Untraceability. In our scheme, all HESs can obtain R and t stored in DBS when they need them. Thus, the adversary can no longer determine whether the user has logged in, by comparing the stored set of each HES. Moreover, messages m_1, m_2 transmitted in public channel are diverse from each other.

5.2.5. Privacy Protection. In our new scheme, we add the server's secret key x and make slight changes when calculating R and Q. Thus, the adversary can no longer recover user's privacy information through data in DBS. The proposed scheme can provide user privacy protection.

6. Performance Comparison

Various anonymous authentication schemes have been presented in recent years. In this section, we choose a few schemes that use only hash functions and compare them with our scheme in terms of execution efficiency.

We define the execution time of one hash operation is 0.13 μs according to Ref. [36]. The number of hash operations of each scheme is shown in Table 4. Since the subscription phase and hand-off phase are similar with the issue phase, we only compare hash operations in the initialization phase and issue phase.

From Table 4, our scheme performs better in terms of execution time. Moreover, the number of parameters transmitted on public channel is minimal, which means our scheme performs better in computing storage. In order to

show the comparison of execution efficiency more clearly, we show the execution time in μs and parameter numbers in Figure 7. It is obvious to see that our scheme has the shortest execution time under the same conditions.

7. Conclusion

The security of pay-TV systems is facing the challenge of explosive growth of users and service content. To prevent unauthorized access in mobile pay-TV systems, anonymous authentication technologies are commonly used for secure media delivery and channel protection. In this paper, we review Far and Alagheband's protocol and find that this protocol is suffering from risks of revealing user's privacy. Besides, there is still room for improvement in storage. We alleviate the security risks of Far and Alagheband's protocol. Our improved scheme can resist stored set attack and user traceability attack. Performance comparison shows that our scheme performs better in terms of execution time and storage, which means it is suitable for resource-constrained devices in edge computing environment.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant 61872449).

References

[1] N. L. Rayan and K. Chaitanya, *A survey on mobile wireless networks*, International Journal of Scientificand Engineering Research, 2014.

[2] M. Armstrong, "Competition in the pay-TV market," *Journal of the Japanese and International Economies*, vol. 13, no. 4, pp. 257–280, 1999.

[3] A. Zakerolhosseini and M. Nikooghadam, "Secure transmission of mobile agent in dynamic distributed environment," *Wireless Personal Communications*, vol. 70, no. 2, pp. 641–656, 2013.

[4] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[5] S. Yangui, P. Ravindran, O. Bibani, R. H. Glitho, and P. A. Polakos, *A platform as-a-service for hybrid cloud/fog environments*, IEEE International Symposium on Local and Metropolitan Area Networks, Rome, Italy, 2016.

[6] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2018.

[7] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[8] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's Law in Passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[9] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[10] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.

[11] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified Biometric Privacy Preserving Three-factor Authentication and Key Agreement for Cloud-assisted Autonomous Vehicles," *IEEE Transactions on Vehicular Technology*, p. 1, 2020.

[12] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[13] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[14] R. Kumaravelu, R. Sadaiyandi, A. Selvaraj, J. Selvaraj, and G. Karthick, "Computationally efficient and secure anonymous authentication scheme for IoT-based mobile pay-TV systems," *Computational Intelligence*, vol. 36, no. 3, pp. 994–1009, 2020.

[15] S. B. Far and M. R. Alagheband, "Analysis and improvement of a lightweight anonymous authentication protocol for mobile pay-TV systems," in *9th International Symposium on Telecommunications (IST)*, pp. 466–473, 2018.

[16] *Conditional-access broadcasting system*, ITU-R Rec, 1992, https://www.itu.int/rec/R-REC-BT/en.

[17] W. T. Zhu, "A cost-efficient secure multimedia proxy system," *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 1214–1220, 2008.

[18] O. Pal and B. Alam, "Efficient and secure conditional access system for pay-TV systems," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18835–18853, 2019.

[19] V. Kumar, R. Kumar, and S. K. Pandey, "An effective and secure key management protocol for access control in pay-TV broadcasting systems using theory of numbers," in *In proceedings: International Conference on Computing Applications in Electrical & Electronics Engineering (ICCAEEE 2019)*, pp. 369–379, 2020.

[20] Y.-L. Huang, S. Shieh, F.-S. Ho, and J.-C. Wang, "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems," *IEEE Transactions on Multimedia*, vol. 6, no. 5, pp. 760–769, 2004.

[21] S.-Y. Wang and C.-S. Laih, "Efficient key distribution for access control in pay-TV systems," *IEEE Transactions on Multimedia*, vol. 10, no. 3, pp. 480–492, 2008.

[22] H.-M. Sun, C.-M. Chen, and C.-Z. Shieh, "Flexible-pay-per-channel: a new model for content access control in pay-TV broadcasting systems," *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 1109–1120, 2008.

[23] S. F. Yeung, J. C. S. Lui, and D. K. Y. Yau, "A multikey secure multimedia proxy using asymmetric reversible parametric sequences: theory, design, and implementation," *IEEE Transactions on Multimedia*, vol. 7, no. 2, pp. 330–338, 2005.

[24] L. Yeu and J. Huang, "A conditional access system with efficient key distribution and revocation for mobile pay-TV systems," *Acm Transactions on Multimedia Computing*, vol. 9, no. 3, pp. 18:1–18:20, 2013.

[25] A. Rial, "A conditional access system with revocation for mobile pay-TV systems revisited," *Information Processing Letters*, vol. 147, pp. 6–9, 2019.

[26] H. Xiong, Y. Bao, X. Nie, and Y. I. Asoor, "Server-aided attribute-based signature supporting expressive access structures for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1013–1023, 2020.

[27] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional Privacy Preservation in IoV," *IEEE Systems Journal*, pp. 1–12, 2020.

[28] N. Lee, C. Chang, C. Lin, and T. Hwang, "Privacy and non-repudiation on pay-TV systems," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 20–27, 2000.

[29] R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 408–413, 2003.

[30] H. Roh and S. Jung, "An authentication scheme for consumer electronic devices accessing mobile IPTV service from home networks," in *In proceedings: IEEE International Conference on Consumer Electronics (ICCE 2011)*, pp. 717-718, 2012.

[31] J.-H. Yang and C.-C. Chang, "An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers and Security*, vol. 28, no. 3-4, pp. 138–143, 2009.

[32] T.-H. Chen, Y.-C. Chen, W.-K. Shih, and H.-W. Wei, "An efficient anonymous authentication protocol for mobile pay-TV," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1131–1137, 2011.

[33] H. Kim and S. W. Lee, "Anonymous Authentication Protocol for Mobile Pay-TV System," in *Communications in Computer and Information Science*, vol. 339, p. 471, Springer, Berlin, Heidelberg, 2012.

[34] H.-M. Sun and M.-C. Leu, "An efficient authentication scheme for access control in Mobile pay-TV systems," *IEEE Transactions on Multimedia*, vol. 11, no. 5, pp. 947–959, 2009.

[35] H. Wang and B. Qin, "Improved one-to-many authentication scheme for access control in pay-TV systems," *IET Information Security*, vol. 6, no. 4, pp. 281–290, 2012.

[36] H. Arshad, M. Nikooghadam, S. Avezverdi, and M. Nazari, "Design and FPGA implementation of an efficient security mechanism for mobile pay-TV systems," *International Journal of Communication Systems*, vol. 30, no. 15, 2017.

[37] X. Liu and Y. Zhang, "A privacy-preserving acceleration authentication protocol for mobile pay-TV systems," *Security and Communication Networks*, vol. 6, no. 3, 372 pages, 2013.

[38] M. S. Farash and M. A. Attari, "A provably secure and efficient authentication scheme for access control in mobile pay-TV systems," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 405–424, 2016.

[39] W.-C. Kuo, H.-J. Wei, and Y.-H. Chen, "An enhanced secure anonymous authentication scheme based on smart cards and biometrics for multi-server environments," in *2015 10th Asia Joint Conference on Information Security*, Kaohsiung, Taiwan, 2015.

[40] H.-L. Wu, C.-C. Chang, and C.-Y. Sun, "A secure authentication scheme with provable correctness for pay-TV systems," *Security and Communication Networks*, vol. 9, no. 11, 1588 pages, 2016.

[41] H. Zhu, "A simplified deniable authentication scheme in cloud-based pay-TV system with privacy protection," *International Journal of Communication Systems*, vol. 32, no. 11, p. e3967, 2019.

[42] Y. Lindell, "Anonymous Authentication," *Journal of Privacy and Confidentiality*, vol. 2, no. 2, pp. 35–63, 2011.

[43] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, *Investigations of power analysis attacks on smartcards*, Smartcard 1999, Illinois, USA, 1999.