Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 147320, 13 pages
http://dx.doi.org/10.1155/2015/147320

*Research Article*

# IPTV Service Framework Based on Secure Authentication and Lightweight Content Encryption for Screen-Migration in Cloud Computing

**Aymen Abdullah Alsaffar, Young-Rok Shin, and Eui-Nam Huh**

*Department of Computer Engineering, College of Electronic and Information, Kyung Hee University, Republic of Korea*

Correspondence should be addressed to Eui-Nam Huh; johnhuh@khu.ac.kr

Received 12 April 2015; Revised 24 September 2015; Accepted 22 October 2015

Academic Editor: Marco Roccetti



These days, the advancing of smart devices (e.g. smart phones, tablets, PC, etc.) capabilities and the increase of internet bandwidth enables IPTV service provider to extend their services to smart mobile devices. User can just receive their IPTV service using any smart devices by accessing the internet via wireless network from anywhere anytime in the world which is convenience for users. However, wireless network communication has well a known critical security threats and vulnerabilities to user smart devices and IPTV service such as user identity theft, reply attack, MIM attack, and so forth. A secure authentication for user devices and multimedia protection mechanism is necessary to protect both user devices and IPTV services. As result, we proposed framework of IPTV service based on secure authentication mechanism and lightweight content encryption method for screen-migration in Cloud computing. We used cryptographic nonce combined with user ID and password to authenticate user device in any mobile terminal they passes by. In addition we used Lightweight content encryption to protect and reduce the content decode overload at mobile terminals. Our proposed authentication mechanism reduces the computational processing by 30% comparing to other authentication mechanism and our lightweight content encryption reduces encryption delay to 0.259 second.

## 1. Introduction

Currently, IPTV service is attracting consumers and gaining rapid growth for offering diversity of services such as quality of services (QoS) and experience (QoE), security, interactivity, and reliability [1] and delivers a high quality of multimedia contents to consumer's resident through wired set-top box (STB). It distributes television content across IP based network that permits more customized and interactive user experience [2].

The IPTV market has grown rapidly in recent years, in terms of the number of subscribers as well as investment made by service providers [3, 4]. According to recent analysis, by the year of 2020, the number of IPTV subscriptions in the 27 countries of the EU is set to reach 3 times its current size. The IPTV global subscriber base has now passed 50 million customers [5].

The continuous increase of internet bandwidth speed, advancing of smartphone technologies, and advancing of cloud computing capabilities (e.g., storage, bandwidth, and performance) enable consumers to access the internet through variety of networks (e.g., AP, 3G, LAN, WiFi, and LTE) using diversity of devices. The rapid development of this technology is providing consumers with access to the Internet anytime, anywhere in the world, to receive multimedia contents (e.g., video, audio, voice, and photo) and use a diversity of services through cloud computing.

The rapid growth of subscriber for this service encourages service provider to provide IPTV services via mobile terminal to variety of devices (e.g., smartphone, PC, and smart tablet) which provide flexible and secure way to freely move between terminals. User at home can migrate (e.g., pairing) their devices to their set-top box (STB) using WiFi/LAN and receive services anywhere at their home. However, when

users migrate their device to STB at home via access point or via base station outside home, providing secure authentication for user devices and protection to multimedia content when moving between different mobile terminals is critical issue.

Therefore, a framework of IPTV services based on secure authentication and lightweight content encryption for screen-migration in cloud computing is proposed. Our contribution is as follows.

(i) Our proposal provides fast efficient method for migrating variety of user devices to home STB conveniently to receive IPTV services at home and outside.

(ii) Our proposal provides secure registration and authentication to user STB without the need to be at home in order to receive/watch IPTV services.

(iii) Our proposal provides protection to service and content by utilizing DRM which protect the IPTV content from being misused and DCAS which prevent unauthorized receiving of IPTV services.

(iv) Our proposal provides lightweight encryption method to encrypt content when user moves between mobile terminals.

(v) Our proposal provides efficient way to reduce the cost of authentication and delay in interdomain and intradomain.

The secure authentication is provided by using user device unique identification ID and password generated during registration process. The created session and the exchanged messages between user devices and STB are protected by using one time cryptographic nonce during authentication process. Cryptographic nonce guarantees that previously used session cannot be used again and exchanged message cannot be fragged. In addition, we used lightweight encryption to reduce decoding overload at terminals and protect the content [6]. Furthermore, Downloadable Conditional Access System (DCAS) prevents unauthorized receiving of IPTV services and Digital Right Management (DRM) protects digital contents from being misused.

The rest of this paper is organized as follows. In Section 2, we describe the related work. In Section 3, we describe motivated scenario. In Section 4, we describe our proposed mechanism. In Section 5, we explain the performance analysis. In Section 6, we explain our numerical results. In Section 7, we summarize our conclusion.

## 2. Related Work

In [3], the author introduces IPTV architecture, trends, and challenges as well as mobile IPTV deployment challenges and solution. The ITU-T Focus Group on IPTV states numbers of security requirements such as content security, service security, network security, terminal security, and subscriber security [7, 8]. In [9], the author raises the interest and the concerns of mobile IPTV including the status of standard activities when deploying IPTV services over wireless and mobile networks. Secure authentication for user devices over wireless environment and the protection of multimedia are very important issues to guarantee QoS and provide secure environment for user devices and service. In addition, lightweight encryption to reduce the overhead in mobile terminal is important to reduce the long delay which occurs in mobile terminal.

Unlike wired environment, the wireless one introduces many security threats to both user service and multimedia content. For example, wireless communication takes place via the air using radio frequencies and that generates the risk of interception which is a greater threat [10]. Some of these threats aim to crack down integrity of information and reliability of network as well as confidentiality of information [11]. These threats can attack the network and damage the performance of network capacity and streaming quality which provide poor QoS, QoE long authentication delay, and long multimedia delivery delay. In [12], the authors develop a Markovian framework that investigates several important issues related to network capacity and streaming quality in wireless home network.

Many researchers introduce a framework of IPTV where they focus their research on the following areas: delivering IPTV services, integrating technology to IPTV service and new future, improving traditional cable TV operators, and providing new techniques to deliver rich multimedia to IPTV users. In [13] the authors proposed a delivery framework for IPTV service over an IP based WiMAX network at MAC and physical layer. They first introduce the changes that face the delivery of IPTV service over wireless area and then proposed solution to these challenges. The authors claim that using WiMAX can offer high QoS at high data rate for networks. Furthermore, it can be delivered to different regions and remote locations. In [14] the authors proposed policy based service overlay IPTV framework for open strategy. The author set some requirements for Open IPTV design. One of the requirements state that Open IPTV will give the subscriber the freedom to select an EPG freely on service overlay network. Furthermore they can change a service provider easily with personal policy decision in Open TV. In [15] the author proposed analyses of a novel IPTV framework for cable TV operators. The proposed solution is based on combining IP and HFC network. Through their analysis the author tries to provide efficient and economical way to deliver TV programs and even add advanced novel interactive feature such as video on demand (VoD). By enhancing the traditional cable TV operator with these features, the number of subscribers increases and the service is more attractive to others. In [16] the author proposed a rich media framework for communication broadcasting coverage IPTV which aims for portability and performance. They provide hybrid IPTV with efficient application interface and sophisticated media processing as its feature. They claim that the media interface is able to develop rich media run time. Our proposed frameworks aim to provide protection to multimedia content and service protection using well-known techniques such as DCAS and DRM in IPTV environment, provide support to user to connect many different devices through STB at home and wireless communication outdoors which give the user the freedom to access the IPTV service from any place at any

time, and provide lightweight encryption not only to protect multimedia content but also to reduce the overhead in mobile terminal. The features in our framework are not clearly and widely discussed in previous works.

In [17] the authors proposed viewer identification and authentication in IPTV using RFID technique where they connected RFID system with IPTV STB. Subscriber is identified and authenticated by using RFID tag wirelessly. The RFID tag stores subscriber viewing rights/service subscription rights that enable them to view the agreed-on services. In [18] the authors proposed secure user authentication scheme by using smart cards in IPTV or by using smart card with bioinformation to ensure strong security and secure authentication. Their scheme aims to provide contents to subscribers according to subscriber attribute. In [19] the authors proposed secure authentication approach based on Kerberos for M2M Open IPTV system where they introduce key distribution based Kerberos. The authors claim that their proposal provides an efficient authentication process and secure content transfer among users as well as decreasing authentication time. In [20] the author proposed a secure mutual authentication for IPTV broadcasting. They use key exchange scheme between STB and smart card for IPTV broadcasting. The scheme relays on set of attributes to authentication user which are generated during registration process without revealing the identity of user. They claim that their proposal provide strong security against common threats in the IPTV environment.

A strict authentication process might generate long overhead to the system and simple authentication mechanism might be barely enough to provide the minimum security requirement. Similar to our approach, other research efforts have been made to provide secure authentication for user devices and protect multimedia content over wireless environment. However, to the best of our knowledge they do not consider mobile terminal overhead which results from encrypting all the content that leads to degrading the QoS, increases in migration delay, and poor QoE. We proposed lightweight encryption which only encrypts part of the content (see Section 4.2.2). By using a partial encryption characteristic of H.264, it is enough to protect the digital content [21] as well as reduce the overhead in mobile terminal which is not considered by other works.

*2.1. DCAS and DRM in IPTV Security System.* In present, multimedia has been digitalized and uploaded to the Internet for easy access anywhere anytime. DCAS is used to ensure that only subscribed member can receive services. The downloaded CA code via the secure DCAS network is supposed to be unhackable and it can prevent illegal subscriber from accessing digital contents. DCAS benefits provide greater and more dynamic security, which is more flexible and easier to manage. It can be applied to variety of devices including a secure microprocessor chip [22].

DRM protects digital content right to ensure it is not compromised (e.g., editing, copying, and reproducing). Encryption of data, certified users license, and secure terminals are necessary to control contents and prevent illegal copies. It is only when the requirements of use are presented that the decryption is executed [23]. Universal DRM such as ISMA and Microsoft is used to encrypt all content [24].

*2.2. Kerberos.* Kerberos is a well-known authentication mechanism which uses centralized servers. A third-party authentication server is used to allow users and servers to trust each other for establishing secure communication. Symmetric encryption for authentication is used to encrypt data [25, 26]. The drawbacks are that (1) user accesses workstation and pretends to be someone else and (2) replay attack might occur when a user eavesdrops on exchanges and gains access to server [26]. Previously, Kerberos was used as authentication mechanism but, for its weakness in security, it is not secure enough against the security threats which we discussed in Section 1.

*2.3. Anonymity and Privacy Assurance.* It is a well-known authentication mechanism that uses Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication along with symmetric key (PKI). A single sign on (SSO) allows user to log in only once and use service without further authentication [25]. Anonymity is used for user security and provides an easy exchange session key. The security of TLS is strong; however, certification overhead of client side is its strong weakness [25]. The drawback of SSO is that user may access many resources once authenticated. This increases the negativity impact in case the credentials are available to other persons and misused which is critical weakness [27].

*2.4. H.264 Description.* Most of the current digital contents are encoded using many standard methods. H.264 is a very high compression rate which is used for digital video CODEC. H.264 has NAL (Network Abstract Layer) which consists of header and Raw Byte Sequence Payload (RBSP). The NAL has unit types that can be distinguished through header and RBSP which corresponded to compressed video data or header information data [24]. Figure 1 shows sequential NAL units which are transmitted through the network.

NAL units consist of many types such as Sequence Parameter Sets (SPS), Picture Parameter Set (PPS), and Pictures. SPS is one of the NAL types which include information such as the number of reference frames and resolution. NAL bits consist of a number of sequences in a bit sequence of H.264 streams. Figure 2 illustrates the relation among the types of NAL unit in bit sequence [24].

*2.5. Cloud Computing.* A cloud is a type of parallel and distributed systems consisting of a collection of interconnected and virtualized computers [28]. It provides shared pools of configurable IT resources (e.g., processing, network, software, information, and storage) on demand, as a scalable and elastic service. Major advantages are software as a service (SaaS), utility computing, network service, platform as a service (PaaS), management service provider (MSP), commercial service platforms, integrating Internet, and highly elastic and optimized utilization of computing resources [28].

Table 1: Table system parameters.

| Notation | Description |
|---|---|
| $ID_M$ | Unique mobile identity generated during registration process. |
| $ID_{PW}$ | Unique password of user mobile generated during registration process. |
| $Lic_M$ | License of user mobile generated based on the service agreement. |
| $STB_N$ | Model number of set-top box which is used to identify it. |
| $STB_{ID}$ | Unique identity of set-top box generated during registration process. |
| $STB_{PW}$ | Unique password of set-top box generated during registration process. |
| $STB_{Lic}$ | License of set-top box generated based on the service agreement. |
| $Nonce_M$ | Arbitrary number of user mobiles that may only be used once. |
| $Nonce_{STB}$ | Arbitrary number of user STB that may only be used once. |
| $Nonce_{SP}$ | Arbitrary number of service providers that may only be used once. |
| $E_{CT}$ | Encrypted digital content using lightweight encryption method (Section 4.1.2). |
| $D_{Nonce}$ | Arbitrary number of Kerberos servers that may only be used once. |
| Nonce | Arbitrary number of Kerberos clients that may only be used once. |

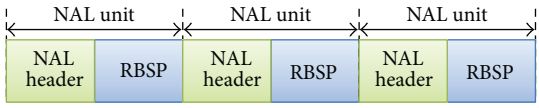


Figure 1: Sequence of NAL unit.

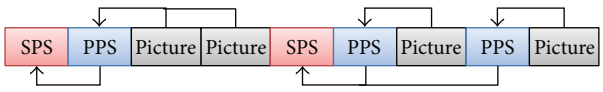


Figure 2: Relation among the types of NAL unit.

## 3. Service Scenarios

Our service scenario consists of two parts as it is shown in Figure 3. The first part starts when user wants to migrate their devices to STB at home to receive IPTV service. The users first register their devices through IPTV service and then use their information to migrate to their STB at home. In this case the user can be anywhere inside their house and still receive IPTV services. For example if the user is interested in cooking show, they can in advance prepare the ingredients for cooking and learn how to cook certain food in real time.

The second part starts when users are outside home and need to migrate their devices to STB via base station. The user can connect their devices to their STB for any kind of purpose such as being on time to watch their favorite show, drama, movie, and soccer games.

## 4. Proposed Mechanism

In this section, we present our proposed mechanism which consists of two parts. In the first part, we describe our secure authentication mechanism when migrating user devices to STB via access point at home and via base station outside home (see Figure 3). The users have to register their devices and then preform authentication when migrating to STB. In the second part, we present our method using lightweight content encryption for mobile device. Table 1 describes parameters of system.

*4.1. Security Framework for Mobile IPTV.* In this section we describe secure registration and authentication process for user smart device when they migrate to STB via access point at home and via base station outside home.

*4.1.1. Registration Process to Migrate User Mobile to STB via Access Point.* We assume that the user only can receive IPTV services through their STB at home where they can watch movie or drama only by using TV. Therefore, we will register and authenticate user mobile for the first time through their STB. By connecting mobile devices to STB through AP or STB with built-in WiFi technology [1] they can perform secure registered and authenticated process as it is illustrated in Figure 4.

*(a) System Sequence Diagram.* The following components of this environment are defined in this paper:

(i) User Mobile and STB store a unique USIM that contains user personal information (e.g., id, password, and user content license for mobile). It can generate random number (Nonce) used for user identity verification. It also makes sure that a previous session is not used again.

(ii) Wireless access point (AP) provides access between STB and users devices at home.

(iii) Service provider (SP) provides IPTV services to consumer mobile devices at home or outside (e.g., indoor and outdoor).

(iv) Database (DB) stores all consumers' information and updates them as needed.

(v) License provider (LP) generates a license for consumer home STB or mobile devices.

(vi) Content provider (CP) provides and prepares the content based in the agreed license.

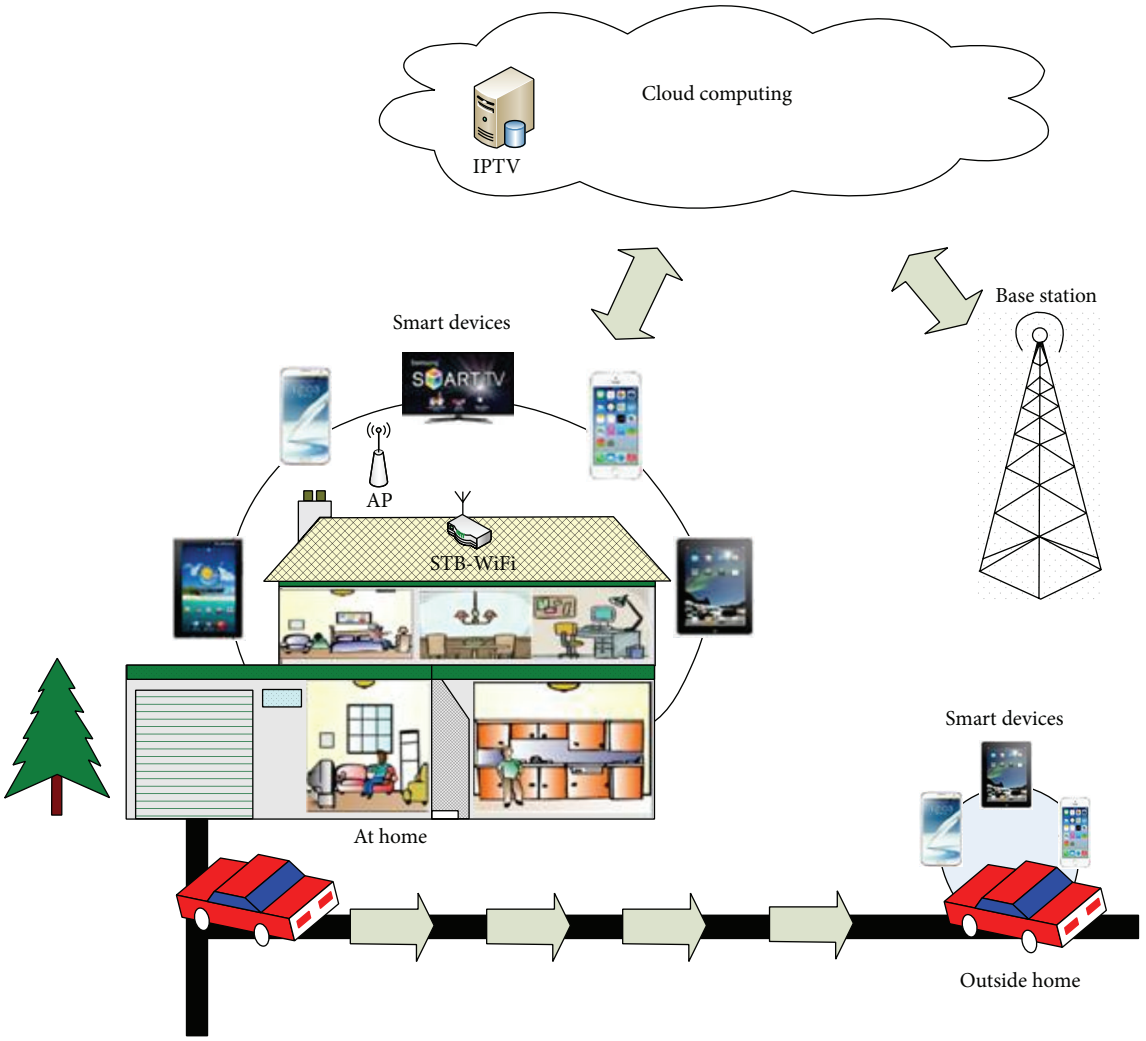


Figure 3: Service scenario.

*(b) Authentication Process*. When a new user subscribes to the subscribed programs with their mobile device, they send a request through AP to STB at home so they migrate their devices to STB followed by mobile generated random number ($Nonce_M$) to prevent security threats such as man-in-the-middle attack from occurring. Then the user STB requests from mobile devices the following information such as $\{ID_M \mid STB_N \mid STB_{ID} \mid STB_{PW}\}$ followed by mobile received random number ($Nonce_M$) and STB generated random number ($Nonce_{STB}$) in order to authenticate and authorize the user mobile device to gain access to user STB at home. After computing, it will look like the following:

(i) Mobile user sends request $\{Req \mid Nonce_M\}$.

(ii) STB request $\{ID_M \mid STB_N \mid STB_{ID} \mid STB_{PW} \mid h(Nonce_M \mid Nonce_{STB})\}$.

(iii) Mobile user sends $\{ID_M \mid STB_N \mid STB_{ID} \mid STB_{PW} \mid h(Nonce_M \mid Nonce_{STB})\}$.

The STB received requested information and compared it with that stored inside STB smart card (USIM). If it is valid, then it transmits it to service provider. Otherwise, an error message is send to mobile device.

*(c) Registration Process*. When mobile user authentication and migration to STB is completed, it transmits $\{ID_M \mid STB_N \mid STB_{Lic}\}$ to service provider where it forwarded information and completed user mobile registration. After that a request is forwarded to database and to the license to update user information and generate a new license for user mobile, respectively. After computing, it will look like the following:

(i) $\{ID_M \mid STB_N \mid STB_{Lic}\}$.

*(d) Generation of License Process*. When a license provider receives $\{ID_M \mid STB_N \mid STB_{Lic}\}$ from service provider, it will generate another license for $\{Lic_M\}$ and forward one copy to content provider, user STB, and mobile devices. After computing, it will look like the following:

(i) $\{ID_M \mid Lic_M\}$.

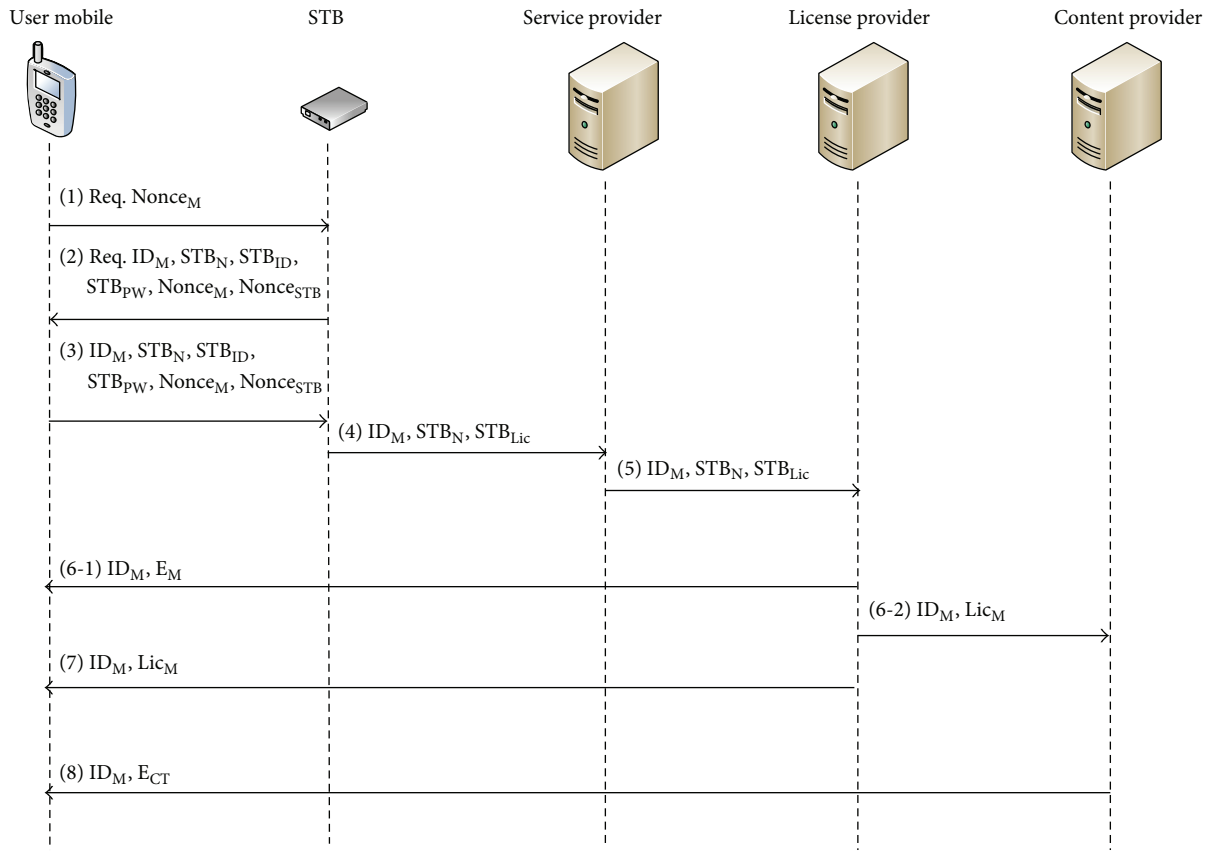


Figure 4: User device registration process to migrate user mobile device to STB through access point.

*(e) Transmit of Content Process*. The content provider receives mobile device license ($Lic_M$) which was generated by license provider. Upon the agreed license, the content provider prepares the suitable content to be played in different devices. The content will be encrypted ($E_{CT}$) using lightweight encryption method (see Section 4.1.2) and transmitted to user mobile through mobile switch center. Finally, the mobile user decrypts the content and watches their programs through their STB and mobile devices.

*4.1.2. Migrate User Mobile to STB via Access Point at User Resident.* We assume that users are watching their program at home and suddenly needed to go out but they still want to move around the house freely. The process of migrating devices to STB through AP has fewer steps than before. We also are assuming that the mobile users have stored license in their mobile device and previously migrated their devices at least once to the STB (see Figure 5).

*(a) System Sequence Diagram*. We briefly describe steps for user to migrate their mobile devices to STB using AP at home. The user connects mobile device to STB through AP where it will compare the received mobile license with stored one in STB. If it is valid, it will transmit user request to content provider where it will prepare content, encrypt it, and transmit it through user STB to mobile user (see Figure 5).

*(b) Process of Migration to STB*. Mobile users connect to STB through AP and send a request to STB to watch the program followed by mobile user random number ($Nonce_M$) to prevent some of the security attacks that we mentioned previously. The STB request $\{ID_M \mid Lic_M\}$ followed by random number ($Nonce_{STB}$) and in return mobile user forwards the requested information. The STB compares $\{ID_M \mid Lic_M\}$ with stored one in STB and forwards the request to content provider. After computing it will look like the following:

(i) Mobile user sends request $\{Req \mid Nonce_M\}$.

(ii) STB request $\{ID_M \mid Lic_M \mid h(Nonce_M \mid Nonce_{STB})\}$.

(iii) Mobile user sends $\{ID_M \mid Lic_M \mid h(Nonce_M \mid Nonce_{STB})\}$.

*(c) Transmit of Content*. The content provider requests a copy of user mobile information that is stored inside user STB such as $\{ID_M \mid Lic_M\}$ and compare it with that stored in content provider for validation. If this is valid then content provider prepares the content to be viewed in different devices and encrypts them to provide services to user mobile. Therefore, the mobile user receives the requested content and enjoys it with their family indoors or in their private time. User mobile will receive error message when received information is not valid.

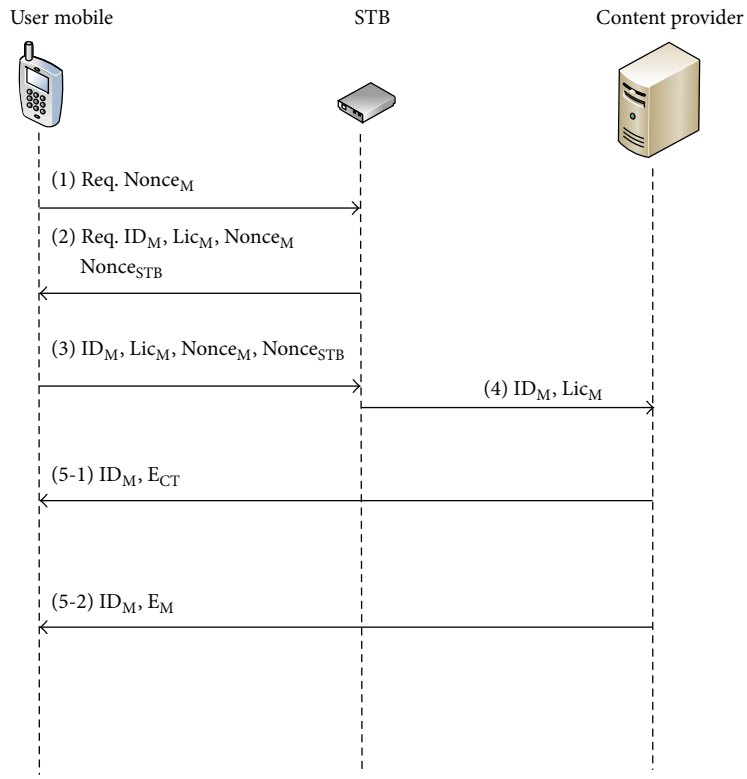


Figure 5: Migrating mobile devices to STB through access point at user resident.

*4.1.3. Migrate User Mobile via Base Station Outside.* We describe the authentication mechanism where users are outside their home and want to receive the IPTV services without the need to connect to STB at home. We assume that the mobile user already has a mobile license to receive IPTV services through mobile terminal to connect to the IPTV services. When user comes home and still wants to view IPTV services privately, then, based on how close they are to STB, the connection will be switched. In other words, when user is nearby STB, then user will receive the services through STB or base station when they are not nearby the STB. Therefore, users will have flexible methods to switch their devices from indoor to outdoor network/environment and vice versa (see Figure 6).

*(a) System Sequence Diagram*. We describe steps for user to migrate their mobile devices to STB using mobile terminal outdoors. Here the mobile users send request through base station to service provider where they request {$ID_M$ | $Lic_M$} from mobile user for validation against stored one in mobile user STB or database. If it is validated a request of service will be sent to content provider, where they prepare the content, encrypt it using lightweight encryption methods (see Section 4.1.2), and then send it to mobile user. If it is not valid, error message will be sent to user mobile rejecting granting the service (see Figure 6).

*(b) Process of Authentication*. For outdoor IPTV services, the users send request to service provider through base station from their mobile devices. In return the service provider requests {$ID_M$ | $Lic_M$} followed by generated random number ($Nonce_M$) from user mobile and service provider ($Nonce_{SP}$) to compare it with stored user information in STB or database. If it is valid, the request is forwarded to content provider to provide IPTV services to user mobile devices. Otherwise, an error message is sent to mobile user to reject granting the services. After computing, it looks like the following:

(i) Mobile user sends request {Req | $Nonce_M$};

(ii) Service provider requests {$ID_M$ | $Lic_M$ | h($Nonce_M$ | $Nonce_{SP}$)};

(iii) Mobile user sends {$ID_M$ | $Lic_M$ | h($Nonce_M$ | $Nonce_{SP}$)}.

*(c) Transmit of Content*. The content provider receives a request from service provider to provide IPTV services to mobile user {$ID_M$ | $Lic_M$}. Then the content provider prepares the content and encrypts it using lightweight encryption methods (see Section 4.1.2) and, finally, transmits it to user mobile to watch it.

*4.2. Multimedia Protection Mechanism.* In this section, we describe mobile DCAS architecture and how user can get the requested digital content after being authenticated. Furthermore, we utilized lightweight content encryption for mobile IPTV service to reduce content overload at terminals.

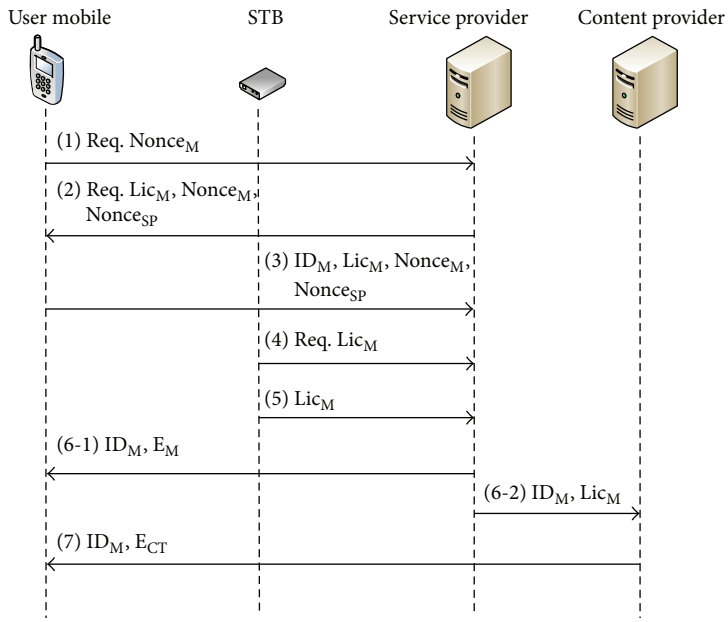


Figure 6: Third phase process of migrating mobile devices to STB through base station.

*4.2.1. Mobile DCAS Architecture.* DCAS architecture consists of server and client side. The consumers send request to Server Authentication to get authenticated. A request is sent to Key Management Server to generate key and transfer to Encryption Algorithms and Content Encryption Algorithm. Content will be sent to Content Encryption Algorithm for encryption and transferred from Streaming Server to Content Decryption Algorithms where encrypted key is used to decrypt the content. Finally, it is viewed by STB or mobile devices (see Figure 7).

*4.2.2. Lightweight Content Encryption for Mobile IPTV Services.* When mobile terminals decode content, many overheads and problems are occurring, since the mobile terminal has limited performances and resources. Therefore, lightweight content encryption technique is proposed where partial encryption technique is applied. By using a partial encryption characteristic of H.264, it is enough to protect the digital content [21]. The light way to encrypt content for mobile terminals is to selectively encrypt important types of NAL unit. SPS is a well-known type of NAL units which is preferred by others to decode the content. First, we start by finding the important NAL units such as SPS. After detecting the important part, only RBSP parts are encrypted in the H.264 bit stream except the header. Figure 8 shows the encrypted part by the proposed technique.

## 5. Performance Analysis

*5.1. Security Analysis.* We consider security issues, communication cost, and handover latency in our performance analysis. A secure authentication and authorization is very critical security issue when migrating mobile devices with other devices through wireless communication. When authenticating the user, a security threat might occur such as the following.

*5.1.1. Denial-of-Service Attack.* It occurs by an attacker to update false verification information for the next login phase in server [29]. For instant, attacker $C$ tries to deceive User $A$ and Server $B$ by intercepting User $A$ login request message $M(\mathrm{ID}, \mathrm{PW})$. Attacker $C$ impersonates Server $B$ and sends the message "access denied" to deceive User $A$. Then attacker $C$ deceives Server $B$ by sending another message $M'(\mathrm{ID}, \mathrm{PW})$ which updates the verification table and stores false verification that causes rejection of all User $A$ login requests.

*5.1.2. Man-in-the-Middle Attack.* It is a form of active eavesdropping between Users $A$ and $B$ communication [30] where the attacker makes independent connection with the victims and relays messages between them. Both users believe they are directly talking to each other over a private connection, when it is run by the attacker.

*5.1.3. Replay Attack.* It is a network attack where transmitted valid data are maliciously repeated or delayed. It is executed by the originator or an adversary who intercepts the data and retransmits it [31].

These security threats' purpose is to acquire access to user's computers or to steal a session during user's communication which compromises user privacy and security. As a result, we utilize cryptographic nonce (number) in user authentication between consumer mobile devices and STB which is used once. It is a pseudorandom number issued to prevent the reuse of old communication [32, 33]. Every time

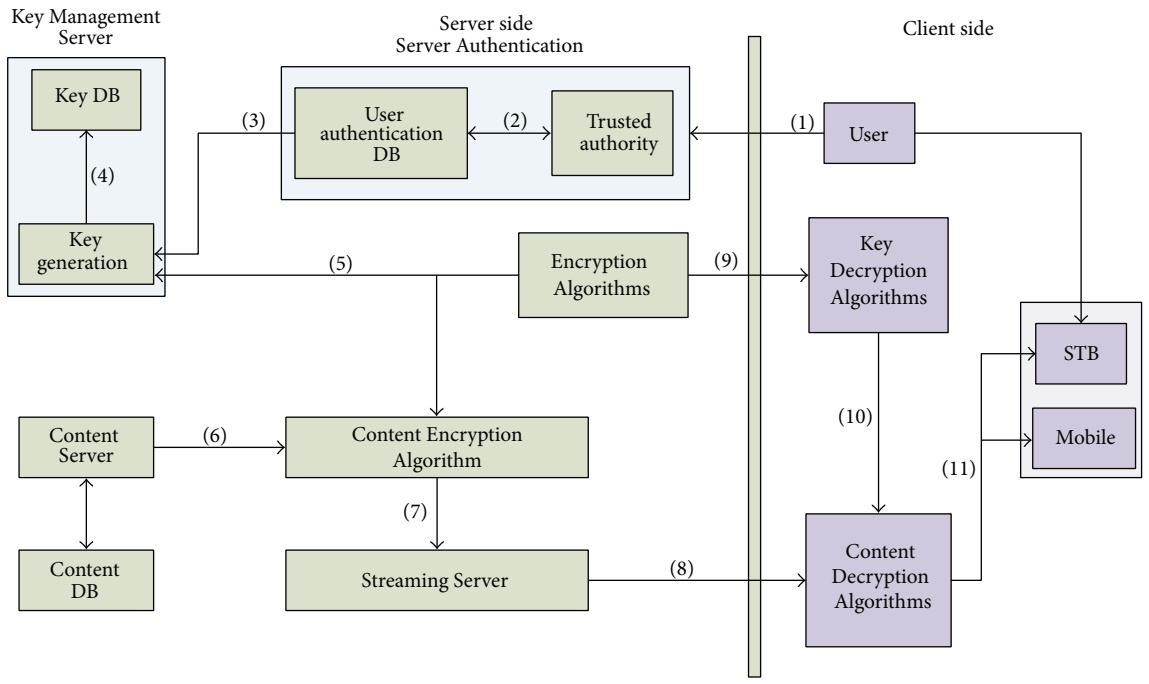


Figure 7: Mobile DCAS architecture.

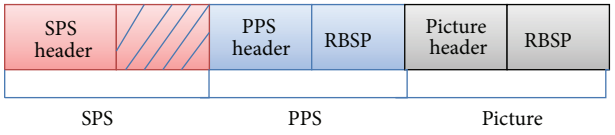


Figure 8: Encrypted part by proposed technique.

the 401 authentication challenge response code is presented, a new nonce will be randomly generated. As a result, client request will have a unique number to prevent other attacks from happening [32].

*5.2. Communication Cost Analysis.* In analysing the cost of proposed authentication mechanism, we will compare it with previously proposed authentications such as Kerberos and EAP-TLS. We will calculate the number of messages exchanged between entities in each authentication mechanism to obtain the cost efficiency [34]. Consider

$$C_{aut\_Msg} = 3C_{M\_STB} + 1C_{STB\_SP} + 1C_{SP\_LP} + 1C_{LP\_CP} + 2C_{M\_LP} + 1C_{M\_CP}. \quad (1)$$

In our proposed authentication mechanism we calculate the cost of exchange messages between all entities where we count the cost of exchange messages between mobile user and STB, STB and service provider, and so on. By computing the authentication partial costs of each step, we can obtain the authentication cost of Kerberos, EAP-TLS, and proposed authentication mechanism. We assume that the delivery cost of a message between mobile users and other entities such as access point, STB, and service provider is mentioned in Table 2 which we used to compute authentication cost in all mentioned mechanisms [35, 36].

Table 2: Authentication cost parameters.

| Symbol | Description | Value |
|---|---|---|
| $C_{M\_STB}$ | Mobile to STB | 1 ms |
| $C_{STB\_SP}$ | STB to service provider | 1.5 ms |
| $C_{SP\_CP}$ | Service provider to license provider | 2 ms |
| $C_{LP\_CP}$ | License provider to content provider | 2.5 ms |
| $C_{M\_LP}$ | License provider to content provider | 3 ms |
| $C_{M\_CP}$ | Mobile to content provider | 3.5 ms |

The proposed authentication mechanism shows more improvement in communication cost compared to other existing authentication mechanisms [37–39]. In Table 3, we are comparing the authentication cost of exchanged messages between existing authentication mechanism, previously

Table 3: Estimation of the authentication cost of Kerberos, EAP-TLS, and proposed authentication mechanism.

| Kerberos | EAP-TLS | Previous work | New proposed mechanism |
|---|---|---|---|
| $2C_{M\_STB} + 2C_{M\_LP} + 4C_{M\_CP} = 22$ ms | $3C_{M\_STB} + 1C_{M\_CP} + 5C_{M\_LP} = 21.5$ ms | $3C_{M\_STB} + 1C_{STB\_SP} + 1C_{SP\_LP} + 1C_{LP\_CP} + 2C_{M\_LP} + 1C_{M\_CP} = 26$ ms | $3C_{M\_STB} + 1C_{STB\_SP} + 1C_{SP\_LP} + 1C_{LP\_CP} + 2C_{M\_LP} + 1C_{M\_PC} = 18.5$ ms |

Table 4: Content specification.

| Component | Description |
|---|---|
| CODEC | H.264 |
| Duration | 00:00:11.96 (11.96 sec) |
| Resolution | 176 × 144 |
| Frame rate | 25 fps |

Table 5: Test environment specification.

| Component | Description |
|---|---|
| Processor | 2.33 GHz Intel Core2 Duo |
| Memory | 3 GB |
| Compiler | Java |
| Operating system | Windows 7 |
| Encryption algorithm | AES-128 |
| Decoding software | FFmpeg |

proposed mechanism, and new proposed one. Our proposed authentication mechanism exhibits greater performance in terms of authentication cost (18.5), compared to the Kerberos (22), EAP-TLS (21.5), and previously proposed (26) authentication procedure. This is caused by the few security operations and exchanged message involved between entities, compared to Kerberos and EAP-TLS.

*5.3. Experiment Setup Environment.* In this section we provide more information about our experiment setup. Table 4 illustrates the content specification which we used in our experiment. It consists of CODEC, duration, resolution, and fps. Table 5 illustrates our test environment specification. In our experiment we used AES128 encryption/decryption algorithm [6].

## 6. Numerical Results

We evaluate the numerical results based on the analysis derived in the previous subsection such as cost authentication, handover latency, and lightweight content encryption results. First we experiment the cost of authentication when we exchange message in the three authentication mechanisms. We define latency as the time it takes a packet to travel from source to destination [37].

Figure 9 illustrates accumulated authentication cost of the exchange messages in Kerberos, EAP-TLS, and proposed authentication mechanism. We assume that the user is authenticated every time consumer gets access to restart IPTV services after turning TV off. As a result, we will use

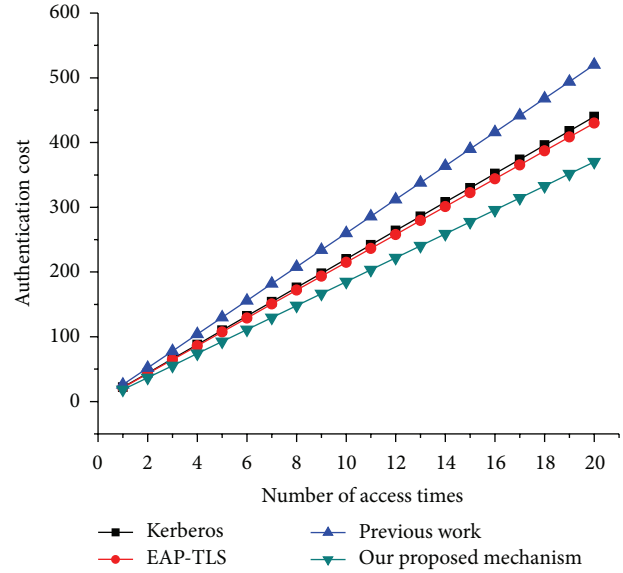


Figure 9: Accumulated authentication cost versus the number of times mobile users access the services.

the number of access times the user attempted and the cost of each authentication mechanism to show the difference of authentication cost between them. Our proposed authentication mechanism not only reduces the authentication cost but also reduces the computational processing and energy cost at the level of mobile devices. For example, we assume that the number of access times the mobile user attempted was 20 times for our proposed authentication mechanism and other authentication mechanisms.

Our proposed authentication mechanism reduces the computational processing and energy cost by 30% compared to other authentication mechanisms. In addition, the reduced number of messages exchanged optimizes the usage of the radio resources enhancing the efficiency of user authentication (see Figure 9).

A continuous switching between indoor and outdoor network/environment might lead to handover latency (see Figure 10) which affects the service of real-time applications of mobile users. Handover latency highly depends on the distance and delay between source and destination [38]. Therefore, a comparison between Kerberos, EAP-TLS, and proposed authentication mechanism is presented. For simplicity, we make the following assumptions: the inter-domain will represent user mobile and STB. The outer-domain will represent service provider, license provider, and content provider. We will compute the number of messages exchanged between these domains and then multiply the

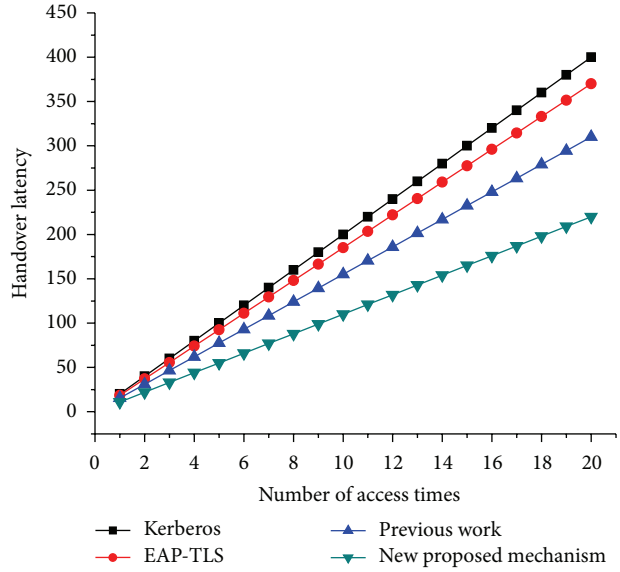


Figure 10: Handover latency versus number of access times.

Table 6: Computing the delay in interdomain and outer-domain in the three authentication mechanisms.

| | Kerberos | EAP-TLS | Previous work | New proposed mechanism |
|---|---|---|---|---|
| Interdomain | 3 msg | 3 msg | 3 msg | 1 msg |
| Outer-domain | 3 msg | 4 msg | 6 msg | 3 msg |
| Total delay (ms) | 20 ms | 18.5 ms | 15.5 ms | 11 ms |

value by the number of times the user performs this process (see Table 6). We did not consider adding the delay value of previously proposed method in [39] because it was not calculated. Note that we are not considering messages exchange within the domain. We use the same parameter values mentioned previously (see Table 2).

*6.1. Lightweight Content Encryption Analysis.* We compared our proposed method E-SPS with E-Entire. Our experiment result shows that E-SPS encrypt content to small size and spend less time for content encryption (0.259 sec). In E-Entire case, E-Entire spends longer encryption time (99.51056 sec). Moreover, the encrypted content could not be decoded very well during decoding process. Figure 11 shows outperforming results using lightweight content encryption introduced in Section 4.1.2.

Figure 12 illustrates secure encryption for content. We can see windows: 2 windows in the top and 2 windows in the bottom. The result shows that the upper windows can play the movies very well without any processing overhead. However, the bottom windows cannot play movies properly even though they are partially encrypted. Therefore, our proposed mechanism shows better performance comparing to others.

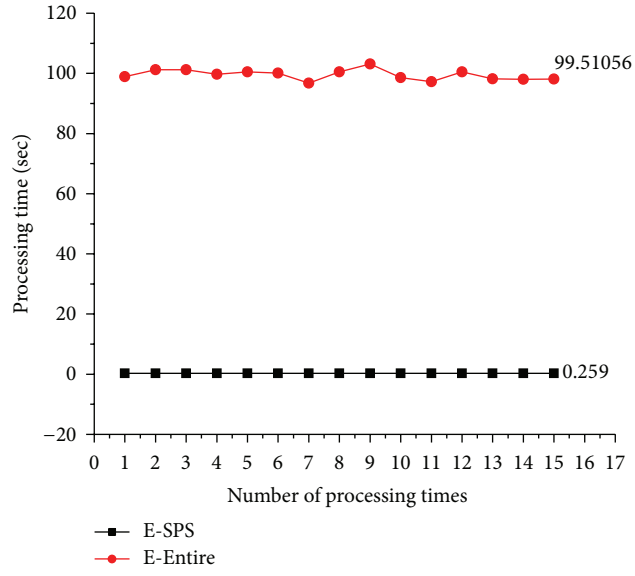


Figure 11: Encryption delay.

## 7. Conclusion

In this paper we presented a framework of IPTV service based on secure authentication and lightweight content encryption for screen-migration in cloud computing. User devices authentication and content protection are considered as a critical issue that should be addressed in wireless network security. Our proposed authentication mechanism eliminates the repeated authentication steps occurring in migration process which improves the performance of user authentication where less security operation and message that are exchanged are used. DCAS is used to protect the service and DRM is used to protect digital content where a lightweight

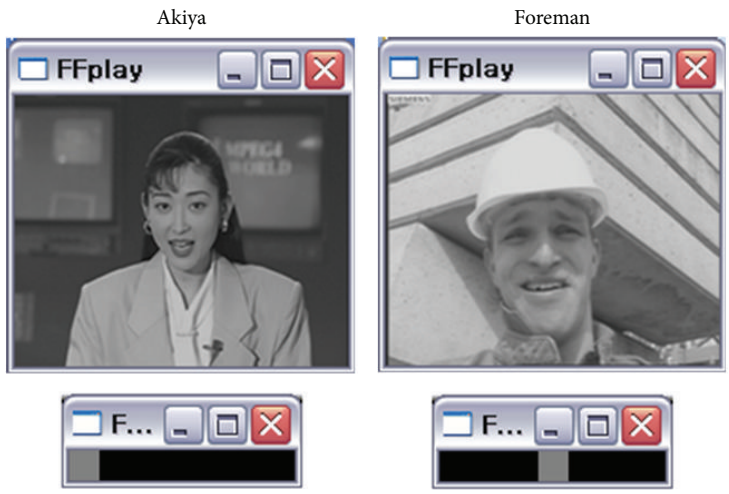


Figure 12: Contents protection.

content encryption with H.264 characteristic is used in digital content protection as well. It reduces the encryption time spent in encrypting content and provides better quality when playing movies. Our result shows decrease in cost and handover latency compared to other authentication mechanisms, which enhances the service quality of real-time applications of mobile users.

## Conflict of Interests

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

## Acknowledgment

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea Government (MSIP) (B0101-15-0535, Development of Modularized In-Memory Virtual Desktop System Technology for High Speed Cloud Service).

## References

[1] D. Ramirez, *IPTV Security: Protecting High Value Digital Content*, John Wiley & Sons, London, UK, 2008.

[2] IPTV, http://en.wikipedia.org/wiki/IPTV.

[3] Cryptographic Nonce, https://en.wikipedia.org/wiki/Cryptographic_nonce.

[4] Cryptographic and Data Security, http://www.tcs.hut.fi/Studies/T-79.159/slides/lecture11.pdf.

[5] M. Gouda and M. Haggag, "Enhanced authentication mechanism for next generation networks," in *Proceedings of the 1st International Conference on Computational Intelligence, Communication Systems and Networks (CICSYN '09)*, pp. 288–295, IEEE, Indore, India, July 2009.

[6] Y.-R. Shin, J.-H. Lee, and E.-N. Huh, "Lightweight content encryption technique for mobile IPTV service," in *Proceedings of the 2nd International Conference on Internet (ICONI '10)*, pp. 831–832, December 2010.

[7] J.-D. Choi, S.-H. Jung, Y.-H. Kim, and M.-S. Yoo, "A fast and efficient handover authentication achieving conditional privacy in V2I networks," in *Smart Spaces and Next Generation Wired/Wireless Networking*, vol. 5764 of *Lecture Notes in Computer Science*, pp. 291–300, Springer, Berlin, Germany, 2009.

[8] Y.-H. Jung and S.-H. Oh, "Design and implementation of efficient DRM system for content streaming based on H.264," *Journal of the Korea institute of Information Security and Cryptology*, vol. 19, no. 2, pp. 155–162, 2009.

[9] Latency on a Switched Ethernet Network, http://www.rugged-com.com/pdfs/application_notes/latency_on_a_switched_ethernet_network.pdf.

[10] M.-K. Choi, R. J. Robles, C.-H. Hong, and T.-H. Kim, "Wireless network security: vulnerabilities, threats and countermeasures," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 3, no. 3, pp. 77–86, 2008.

[11] M. Waliullah and D. Gan, "Wireless LAN security threats & vulnerabilities," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, 2014.

[12] Replay Attack, http://en.wikipedia.org/wiki/Replay_attack.

[13] I. V. Uilecan, C. Zhou, and G. E. Atkin, "Framework for delivering IPTV services over WiMAX wireless networks," in *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT '07)*, pp. 470–475, IEEE, Chicago, Ill, USA, May 2007.

[14] T.-J. Kim, J.-S. Kim, and M.-S. Hahn, "Policy-based service overlay IPTV framework for open strategy," in *Proceedings of the 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC '10)*, pp. 962–966, Beijing, China, September 2010.

[15] X. Yang, "Analyses of a novel IPTV framework for cable TV operators," in *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC '11)*, pp. 321–326, IEEE, December 2011.

[16] M.-Y. Sung, "A rich media framework for communication-broadcasting converged IPTV," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 463–470, 2010.

[17] H. Jabbar, T.-Y. Jeong, J. Hwang, and G.-L. Park, "Viewer identification and authentication in IPTV using RFID technique," *IEEE Transactions on Consumer and Electronics*, vol. 54, no. 1, pp. 105–109, 2008.

[18] E.-A. Jun, J. G. Kim, S. W. Jung, and D. H. Lee, "Extended fingerprint-based user authentication scheme using smart cards in education IPTV," in *Proceedings of the International Conference on Information Science and Applications (ICISA '11)*, pp. 1–7, Jeju Island, Republic of Korea, April 2011.

[19] I. Doh, K.-J. Chae, J.-Y. Lim, and M. Y. Chung, "An improved security approach based on kerberos for M2M open IPTV system," in *Proceedings of the 15th International Conference on Network-Based Information Systems (NBIS '12)*, pp. 754–759, IEEE, Melbourne, Australia, September 2012.

[20] H. J. Yoo, "Secure mutual authentication for IPTV broadcasting," in *Proceedings of the International Conference on ICT Convergence (ICTC '12)*, pp. 96–99, IEEE, October 2012.

[21] C. Ntantogian, I. Stavrakakis, and C. Xenakis, "Reducing the user authentication cost in next generation networks," in *Proceedings of the 5th Annual Conference on Wireless on Demand Network Systems and Services*, pp. 65–72, Garmisch-Partenkirchen, Germany, January 2008.

[22] 60 Million IPTV subscription in the EU by 2020, 2011, http://www.broadbandtvnews.com/2011/09/29/60-million-iptv-subscriptions-in-the-eu-by-2020/.

[23] S. Zeadally, H. Moustafa, and F. Siddiqui, "Internet protocol television (IPTV): architecture, trends, and challenges," *IEEE Systems Journal*, vol. 5, no. 4, pp. 518–527, 2011.

[24] ITU-Focus Group, http://www.itu.int/pub/T-PROC-IPTVFG-2008/en.

[25] S. H. Park, S.-H. Jeong, and C. J. Hwang, "Mobile IPTV expanding the value of IPTV," in *Proceedings of the 7th International Conference on Networking (ICN '08)*, pp. 296–301, IEEE, Cancun, Mexico, April 2008.

[26] M. Mushtaq and T. Ahmed, "P2P-based mobile IPTV: challenges and opportunities," in *Proceedings of the 6th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA '08)*, pp. 975–980, IEEE, Doha, Qatar, April 2008.

[27] T. Guo, C. H. Foh, J. Cai, D. Niyato, and E. W. M. Wong, "Performance evaluation of IPTV over wireless home networks," *IEEE Transactions on Multimedia*, vol. 13, no. 5, pp. 1116–1126, 2011.

[28] X. Wang, B. Wang, and J. Huang, "Cloud computing and its key techniques," in *Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE '11)*, vol. 2, pp. 404–410, IEEE, Shanghai, China, June 2011.

[29] Internet Streaming Media Alliance, *ISMA Encryption and Authentication Specification Ver. 1.1.2005*, 2005, https://en.wikipedia.org/wiki/ISMACryp.

[30] C.-H. Lee and H.-C. Chiu, "Telco IPTV growth strategy in Taiwan," in *Proceedings of the 13th International Conference on Advanced Communication Technology*, pp. 1469–1474, Gangwon-Do, Republic of Korea, February 2011.

[31] L.-H. Zhang, X.-W. Kong, and C. Yang, "Digital rights management independent of terminals in mobile applications," *The Journal of China Universities of Posts and Telecommunications*, vol. 14, no. 1, pp. 32–38, 2007.

[32] J. H. Park, "Subscriber authentication technology of AAA mechanism for mobile IPTV service offer," *Telecommunication Systems*, vol. 45, no. 1, pp. 37–45, 2010.

[33] Y. Jeong, S. Kim, H. Kim, H.-S. Koo, and E. Kwon, "A novel protocol for downloadable CAS," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 3, pp. 1236–1243, 2008.

[34] Kerberos (Protocol), October 2012, https://en.wikipedia.org/wiki/Kerberos_(protocol).

[35] Extensible Authentication Protocol, http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.

[36] Denial of Service Attack, https://en.wikipedia.org/wiki/Denial-of-service_attack.

[37] Man in the Middle Attack, http://en.wikipedia.org/wiki/Man_in_the_middle_attack.

[38] A. Diab and A. Mitschele-Thiel, "Minimizing Mobile IP Handoff Latency," http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.1273&rep=rep1&type=pdf.

[39] A. Abdullah Alsaffar, T.-D. Nguyen, M. M. Islam, Y.-R. Shin, and E.-N. Huh, "An efficient migration framework for mobile IPTV," in *Computational Collective Intelligence. Technologies and Applications: Second International Conference, ICCCI 2010, Kaohsiung, Taiwan, November 10-12, 2010. Proceedings, Part III*, vol. 6423 of *Lecture Notes in Computer Science*, pp. 292–301, Springer, Berlin, Germany, 2010.