International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-36-40.
Available online at http://www.bioinfo.in/contents.php?id=115

DIGITAL CONONTENT DISTRIBUTION SYSTEM FOR SECURE AND FAST MULTIMEDIA BASED ON PARTIAL ENCRYPTION AND GROUP KEY

PAWAR V.R., VIPLAV KUMAR, ANKUR HINGANE AND ANUSHREE YERAWAR

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- vitthalpawar75@gmail.com.

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- There are constantly mounting opportunities on the Internet and civilizing network capability so, Security and fast multimedia distribution has become an important research topic. It is easy to achieve the faster and more secure multimedia distribution through web caching and encryption. It is important to review encryption technique used for multimedia content in view of specific characteristic of multimedia content such as its size. It is modified to use partial encryption based on the multimedia type in order to reduce user alleged latency. In the modified system it is introduced that only authorized users have access to secure multimedia, group key management. On certified group it is enabled to ensure backward and forward secrecy. A more secure and faster multimedia content distribution will be assured by using these techniques.

Citation: Pawar V.R.,et al. (2012) Digital conontent distribution system for secure and fast multimedia based on partial encryption and group key. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-36-40.

Introduction

Digital content electronic commerce has potentially immeasurable distribution channels due to the phenomenal explosion of the Internet. New technologies enabled improved network speed and larger bandwidth, which made possible distribution of “heavier” digital content such as audio and video. [1,3,4]. To ensure new digital markets it is vital to guarantee end-to-end digital content delivery security [2]. Current studies on ensuring web security can be normally divided into studies focusing on implementing a certain type of basic security technique [1,5-7] and studies on application of security techniques for the relevance of web services [3,4,8-11]. A distinctive characteristic of multimedia content is its big data size. Due to bandwidth restrictions this noticeably results in slower transmission to the end user. This latency is provoked in case of secure distribution relating encryption. Since encryption methods initially intended for textual data they are not quite suitable for multimedia content due to its [multimedia] much larger data size. That causes much slower encryption and decryption process, that in turn results in a greater user apparent latency. Current studies on the transmission of digital content focused on the guarantee of safety and effective distribution. However the Ko et al. [12] accented the importance of both secure and fast distribution of digital content by proposing security technique for each group of multilayered structure and deploying caching based on group-layered structure. Given paper will strengthen the proposed architecture in Ko et al. [1,12] by implementing selective key encryption and introducing key manager into multilayered structure. Selective encryption will ensure more efficient and secure encryption for a certain type of data due to the fact it takes into deliberation data precise characteristics. As it has been mentioned earlier multimedia content is usually of big size, and selective encryption improves apparent latency as it encrypts only a portion of a data, therefore user needs to spend less time on decrypting the content. On the other hand introducing key manager will ensure greater security effective key distribution and rekeying while addressing such issues as join and leave operations.

Related work

Security of digital content Encryption methods used nowadays can be largely categorized as symmetric and asymmetric. Due to

inflexibility and relative insecurity of symmetric method where both encryption and decryption is performed using the same key, asymmetric key encryption is more privileged and more widely deployed in web services [13]. The strength of this method is that encryption can be done by any party using publicly accessed public key of the receiver, and then only receiver can decrypt it using his private key [14]. In a public key based web security system, this method is used in broadcast and reception of actual data by forming encryption channel after the certification of the client and server. Since the appearance of public key concept, a number of algorithms were developed newly. Among them RSA and Diffe-Hellman algorithms are more well known and trusted for their demonstrated safety [14]. Encryption methods to guarantee security of digital content transmission include conventional extensively browbeaten SSL (Secure Socket Layer) and its successor TLS that inserts encrypted layerbetween the application layer and transport layer [1,3,7] that involves certification process through a certification authority (CA). In addition to these basic security techniques, there has been a research conducted on application of security techniques, namely Digital Rights Management (DRM). abstractly the protection, distribution of digital content is referred as Digital Rights Management, where the primary responsibilities of DRM system are: 1) secure delivery of content to users; 2) avoidance of unauthorized access; 3) enforcement of usage rules; 4) monitoring of the use of content. To ensure security DRM system employs cryptography (symmetric key ciphers, public key ciphers and digital signatures) [1,2,8]. Group key management is significant in a sense of providing secured multicast of data to a group of authorized users. The group key has to be managed according to forward and backward secrecy. In forward secrecy, a receiver who has already left the multicast group cannot access the current secure communication any more. In backward privacy a new member who has joined the group cannot access the communication sent before it joined the group. To ensure these two properties the group key must be changed on each membership change and redistributed securely to only valid members. This is called group rekeying [16,17]. Pour et al. [16] suggests using hierarchical group key management scheme for secure multicast and growing effectiveness of key distribution in leave operation. That is when a member joins the group after updating the preceding group key in the server, the new key is sent to all existing group members and the contrary value of the new member is sent to subgroup members, when a member leaves the group server just needs to send the contrary value of the leaving member to the subgroups. Development of apparent latency is passed out through implementing web caching and selective (partial) encoding. Web caching allows to distribute the digital content on proxy servers close to the end user so that to ensure faster digital content retrieval. On the other hand selective encoding reduces latency ensuing from encoding/ decoding the digital content. Xiliang et al. [18] provides a inclusive survey of existing methods for selective encoding. The summarized view on selective encryption schemes can be observed in table 1. Selective encryption methods are broadly classified according to the type of data encrypted: image and video. Further the encryption algorithms for each data type are shown. This categorization helps to deploy a more efficient and secure encryption for a particular type of data due to the fact that each type of data has its own specifics. Encoding using undisputed encryption method for different type will not yield as much security as the method mainly targeted as a certain type of data, thus taking into consideration its precise characteristics to ensure highest possible security.

System design

Existing system structure

Fig. 1 presents a original abstract design of the system [12]. The main components are-

1) DCP (Digital Content Provider) is a supplier of DC (Digital Content)
2) DCUG (Digital Content User Group) is a user group, which is supplied by DC. Majority of multimedia users is only concerned in a passive action of download of multimedia content and playing/viewing it at user's browser. However, a thorough encryption al-

gorithm and certification requires a complex process that causes time delay. Thus, it is more preferable to consider the transmission of DC in regard to execution speed; however an adequate security level should also be maintained Due to the fact that DCUG user in original proposed system can be certified in the DCUG, the user certification becomes fast and easy. In addition, an effect of the Internet traffic of DC in the proposed system decreases, and the execution speed increases due to the fact that the system will be directly affected by the DCUG cache[1].

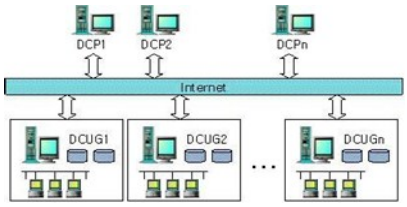

Fig. 1- System Structure

Modified System structure

This paper however proposes adaptation to the original structure by introducing Encryption manager to Digital Content Accelerator and Group-key manager to each authorized DCUG. Figure 3 illustrates the updated configuration of a DCUG. A DCUG is managed by grouping it into two different groups. Digital content accelerator's purpose is to increase user response speed. Introduced encryption manager will implement an suitable selective encryption based on the data type. This is very beneficial because in that case a data type suitable encryption is done, which would guarantee relative security. It can be seen from Figure 2 that two groups can be identified in the DCUG. The first is an certified user group, which has the authority to use encrypted DC, and the second is a user group, without such authority. The second adaptation to original structure proposed in Ko et al. [12] is done to a group of authorized users. The keys used by this group will be handed by the group key manager. In this case, backward and forward secrecy would be ensured, which is vital for multi-user groups. Group-key management is covered in a greater detail in the next section. Fig. 3 presents the cache structure, which is configured by a layered structure. A cache is managed by classifying a caching scope as an authorized user and an unconstitutional user. Therefore, the structural security can be managed in the level of system by separating the DC as an authorized DC and an unconstitutional DC. In

the caching scope of an authorized user, the caching scope can be managed by classifying the DC as an encrypted DC and a widespread DC. In order to implement the right of digital content, an only authorized user can have access to the system. In nowadays marketable systems the user can play-back digital content by receiving an encrypted digital file play-back program, and token. An encrypting method to protect digital content can be classified as a symmetric key method, such as a DES algorithm, and an asymmetric key method, such as a RSA public key algorithm. The existing algorithms meet required conditions to protect digital content, and are widely applied to various systems. In the case of encryption of whole files, which have a large file size, such as video, however, there huge loads are placed on the transmission to the server and network. In addition, the time required for the process of decryption in the execution process of the user is long, and this is a factor in the execution delay. Thus, Ko et al. proposes to use partial encryption, which encrypts a file key and certain core section. However, to ensure safety, it is important to use a safest encryption method for DC transmission from DCP to DCUG. Then for DC stored at DCUG cache the DC can be decrypted and re-encrypted but this time using selective encryption, so that to ensure DCUG user professed latency. Thus security is inversely proportional to execution. In other words, if an encryption ratio is increased, meaning the increased strength of encryption then the execution speed decreases. on the other hand, if the degree of encryption is decreased, the execution speed increases. however, since a safe transmission method, which safely transmits DC using the statement between groups in the DCUG in order to improve these problems, is used it is possible to solve the problem, which includes the lowering of the strength of encryption, due to the partial encryption. [12] The modification to this approach includes selectively encrypting DC based on its type, such as video or image. The specific characteristics of the digital content type imply that for effective selective encryption it is important to a customized encryption for a certain type of data. The list of methods potentially useful for encrypting different types of data is presented.

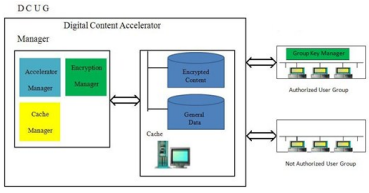

Fig. 2- Updated DCUG Structure

Fig. 3- Cache Structure

Recognition

It can be observed from the Figure 4 how the interface takes place in the system. In case when the authorized user in the DCUG is unable to find the required content in the cache list (cache miss), the DCUG should obtain the content from the suitable DCP server. In this case, the DCUG and DCP servers should issue a certificate by connecting the CA (Certificate Authority) before transmitting and receiving encrypted data for each other.

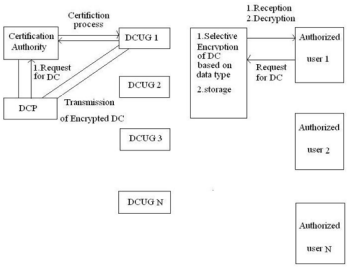

Fig. 4- Overall System Interaction View

DCUG key supervision

If the same key is shared among the DCUG group members it becomes a security weakness in the system. As a further development of [12] idea it is proposed to use a group key for each DCUG. For managing the process of rekeying it is proposed to use hierarchical group key management scheme [16] that would address issue of leave operation. As it was mentioned before the group key has to be managed according to forward and backward secrecy. To ensure these two properties the group key must be changed on each membership change and redistributed securely to only valid members. This is called group rekeying [16]. Pour et al [16] suggests using hierarchical group key management scheme for secure multicast and increasing efficiency of key distribution in leave operation. That is when a member joins the group after updating the previous group key in the server, the new key is sent to all existing group members and the inverse value of the new member is sent to subgroup members, when a member leaves the group server just needs to send the inverse value of the leaving member to the subgroups. Group key is a composition of member secrets and server secrets for each subgroup. On JOIN: new group key is sent through multicast to obtainable members encrypted with previous group key and it is unicast to new member encrypted by its individual key On LEAVE; new key should be encrypted using individual key for each outstanding member and sent through unicast. It is more computationally expensive as with n members there are n connections and encryptions required.

Distributive key management

Pour [16] proposes hierarchical group key management, where the in order to reduce the burden of maintaining the inverse values it proposes to divide the members into subgroups. Since Ko et al. [12] also planned division into subgroups however with different idea in mind, the Pour [16] proposal can be seamlessly integrated into the our planned framework, so that the key manager would be maintained in each DCUG group.

Key generation algorithm

Key generation algorithm to be used in the proposed system is proposed and developed by Pour et al. Further description and explanation is based on Pour et al. original work. [15]

The procedure of rekeying on member JOIN is as follows=

1. On reception of JOIN request, key server authenticates the member. If required, the key server assigns the session key, and sends it to the member.
2. The key server determines the subgroup for the new member and assigns the identity within the subgroup. In this example,

the new member belongs to subgroup 4 and its identity is m. Thus, the path set for subgroup 4 - the keys K4, K3,4 and KG need to be changed.

3. The key server assigns the new member u_4^m a member secret a_4^m and calculates the assigned secret's inverse value a_4^{-m} as well.

4 The key server changes the server secret assigned to subgroup from a_4^s to a_4^{is}

5 The key server updates K4, K3,4 and KG to K'4, K'4 and K'G using a_4^m and a_4^{is} in the following way:

$$K_4^{'} \equiv g^{\alpha_4^1-\alpha_4^{m-1}\alpha_4^m\alpha_4^n}(mod\ p)$$

$$K_{3,4}^{'} \equiv g^{(\alpha_3^1-\alpha_3^m\alpha_4^1)(\alpha_4^1-\alpha_4^{m-1}\alpha_4^m\alpha_4^n)} \text{ (mod p)}$$

$$K_G^{'} \equiv g^{(\alpha_1^1-\alpha_1^m\alpha_1^i)(\alpha_2^1-\alpha_2^m\alpha_2^i)(\alpha_3^1-\alpha_3^m\alpha_3^i)(\alpha_4^1-\alpha_4^{m-1}\alpha_4^m\alpha_4^n)}$$

(mod p)

(in case of 4 subgroups)

6 The key server encrypts {K'4;K'3;4; K'G}, and theinverse values of the other members in that subgroup, $a^{-1}{}_4$, ... a_4^{-m-1} by kp_4^m and sends this encrypted message through unicast to new member u_4^m

S $\xrightarrow{unicast}$

$$\{u_4^m\}:\left[\left(K_4^{'},K_3^{'},K_G^{'},\alpha_4^{-1},\ldots\alpha_4^{-m-1}\right)_{K_{f4}^m}\right]$$

7 Server encrypts a_4^{-m-1}, and K'4 by K4 for subgroup 4, K'3;4 by K3,4 for subgroups 3 and 4, K'G by KG for subgroups 1 to 4, and distributes these encrypted keys through multicast for existing members.

S $\xrightarrow{multicast}$

$$\{existing.members\}:\left\{\left(\bar{\alpha}_4^m,K_4^{'}\right)_{K_4},\left(K_{3,4}^{'}\right),\left(K_G^{'}\right)_{K_G}\right\}$$

In this way, each updated key is encrypted by the previous one for existing members, and as a result, only the members who know the corresponding previous keys can decrypt the encrypted message containing the new keys.

The procedure of rekeying on member LEAVE is as follows:

If u_4^m leaves the group all keys known to this member have to be changed to new: 4 $K_4^{'}$ to 4 $K_4^{''}$, $K_{3,4}^{''}$ to $K_{3,4}^m$ and $K_G^{'}$ to $K_G^{'}$. However there is no need to send each key to the remaining members. Instead the inverse of leaving member's secret (a_4^{-m}) can be used to update the eys. In such case key server prepares one message for subgroup 4 indicating u_4^m has left, and delivers a_4^{-m} for the remaining subgroups (1-3). The value a_4^{-m} is encrypted into multiple copies by K_3 and $K_{1,2}$ for subgroup 3, and subgroups 1 and 2 respectively. The key server sends this message through multicast.

$$S \xrightarrow{mulescon} \{remining.members\}:\{(a_4^{-m})_{k3},(a_4^{-m})_{k1,2}$$

When the remaining members receive this message, they decrypt it by the corresponding keys and the use a_4^{-m} to update those keys.

$$K_4^n \equiv \left(K_4^{'}\right)^{\bar{\alpha}_4^m} \equiv g^{\alpha_4^1-\alpha_4^m\bar{\alpha}_4^m\alpha_4^n} \equiv g^{\alpha_4^1-\alpha_4^{m-1}\alpha_4^n}(mod\ p)$$

$$K_{3,4}^{''} \equiv \left(K_{3,4}^{'}\right)^{\bar{\alpha}_4^m} \equiv g^{(\alpha_3^1-\alpha_3^m\alpha_4^1)(\alpha_4^1-\alpha_4^m\bar{\alpha}_4^m\alpha_4^n)} \equiv g^{(\alpha_3^1-\alpha_3^m\alpha_4^1)(\alpha_4^1-\alpha_4^{m-1}\alpha_4^n)}(mod\ p)$$

$$K_G^{''} \equiv \left(K_{3,4}^{'}\right)^{\bar{\alpha}_4^m} \equiv g^{(\alpha_1^1-\alpha_1^m\alpha_1^i)(\alpha_2^1-\alpha_2^m\alpha_2^i)(\alpha_3^1-\alpha_3^m\alpha_4^i)(\alpha_4^1-\alpha_4^m\bar{\alpha}_4^m\alpha_4^n)}$$

$$\equiv g^{(\alpha_1^1-\alpha_1^m\alpha_1^i)(\alpha_2^1-\alpha_2^m\alpha_2^i)(\alpha_3^1-\alpha_3^m\alpha_4^i)(\alpha_4^1-\alpha_4^{m-1}\alpha_4^i)} \text{ (mod p)}$$

This shifting the responsibility for to users' side improves efficiency of rekeying on leave.

The procedure of rekeying on member JOIN is as Follows:

1. On reception of JOIN request, key server authenticates the member. If required, the key server assigns the session key, and sends it to the member.
2. The key server determines the subgroup for the new member and assigns the identity within the subgroup. In this example, the new member belongs to subgroup 4 and its identity is *m*. Thus, the path set for subgroup 4 - the keys K4, K3, 4 and KG need to be changed.

Analysis and conclusion

The factors, which affect the dispensation speed of a digital content division system, are the delay according to the network traffic, and decryption process in user interfaces. The file size of the original sentence of DC increased due to the encryption. In addition, the encrypted transmission of a large amount of multimedia digital content, such as MP3, appreciably increases the network traffic. The proposed system improves the processing speed by reducing these delay factors. The encrypted content in the DC

server using a public key will be transmitted to the DCUG. The received DC can be decrypted using a personal key, and stored in a cache by applying a partial encryption. Finally, the certified users of the DCUG are supplied DC, which is stored in a cache. Therefore, the traffic on the Internet for the user decreases, and the user will be affected by DC of the DCUG. In addition, because the user interface decrypts a partially encrypted content, the delay time to execute the content decreased.

Table 2. Notation [15]

P	a large prime number
G	A primitive element of multiplicative group $\dot{p}$
I	1,2,..,m,member index
J	1,2,… $\lceil n/m \rceil$, subgroup index,where n is a group size and m is a sub group size
u_j^i	Member i in subgroup j
α_j^i	Member secret assigned to u_j^i ,such that 2≤ α_j^i ≤p-2,ged($\alpha_j^i, p-1$)=1
$\bar{\alpha}_j^i$	Inverse of α_j^i such that $\alpha_f^i \bar{\alpha}_f^i \equiv$ 1(mod p-1)
α_j^5	Server secret for subgroup j such that 2≤ α_j^i ≤p-2
p_j^i	Private key for member i in subgroup j
K	
K_G	Group key shared in the group
K	Subgroup key for subgroup j
$K_{k,l}$	Node key
$\{u_j^i\}$	Set the current users in subgroups
$\{K_f\}_{k_f'}$	K_f is encrypted by K_f^i
$\xrightarrow{unicast}$	Sending data through unicast
$\xrightarrow{multicast}$	Sending data through multicast

A digital content distribution system should be equipped with transmission security and execution security. The DC used in the proposed system safely transmitted the encrypted content to the DCUG using a security verified RSA public key method. Therefore, the proposed system is secure, due to the fact that the DCUG, which has a personal key, can only decrypt the received DC. Because the user in the DCUG should be certified for each group, safety is guaranteed in the DCUG. In addition, the proposed system is secure enough to safely execute contents. The security of the DCUG can be guaranteed by the system itself. The authorized user of the DCUG, who is certified through the user certification, can only be allowed to access the cache list. It is necessary to make decryption when a user interface executes DC, and a certain additional security is guaranteed due to the fact that a single user, who has a proper key, can decrypt the DC. Also the issue of rekeying is addressed on new member JOIN or LEAVE, so that no ensure backward and forward secrecy. Applying hierarchical key management suggests better key management on member LEAVE, and it ensures backward and forward secrecy discussed in the beginning of the paper.

Table 3- Analysis of the proposed system

Issue	Factors	Consideration	Approach of the proposed system
Processing speed	Transmission speed Of the network	Network traffics	Management for each DCUG group/layered structure web caching
	User execution speed	Files size For encryption/ decryption	Layered structure system/partial selective encryption based on file type
Security	Security of the transmission	Safety	Public key method/ management for each group
	Security of the execution	Speed lowering/ Reducing the execution process	Security of the DCUG/ Certification for each DCUG group
	Security on member join/ leave	Ensuring back-ward/ forward secrecy	Hierarchical key management

References

[1] Olga Yugay, Beomjune Kim, Hui-seong Na, Franz I.S. Ko., (2008) *Third International Conference on Convergence and Hybrid Information Technology*.

[2] Eskicioglu A.M., Town J., Delpc E.J. (2003) *Elsevier: Signal Processing: Image Communication* 18, 237-262

[3] Spctral Lines (2001) *IEEE Spectrum*, 38, 6, 9.

[4] Thorwkrth N.J., Horvatic P., Weis R., Jian zhap (2000) *Signals, Systems and Computers*. 2, 1831-1835.

[5] Rivest R., Shamir A. and Adelman L. (1978) *Communications of the ACM*, 21, 2, 120-126.

[6] Korea Information Security Agency (1998) *A Development and Analysis Report on 12bits Block Encryption Algorithm*.

[7] Freier A.O., Karlton P. and Kocher P.C. (1996) *The SSL Protocol Version* 3.0.

[8] DRM Solution, *Secumax:(http://www.secumax.com*).

[9] Siu F. Yeung, John C.S. Lui David K.Y. Yau (2002) 10*th ACM Multimedia*, 392-401.

[10] Perrig A., Song D., Tygar J.D. (2001) *IEEE Symposium on Security and Privacy*.

[11] Just M., Vaudenay S. (1996) *Advances in Cryptology,* 1163, 36-49.

[12] Ko I.K., Yun J.N. (2005) *EUC Workshops*, 1265-1272.

[13] Stallings W. (1999) *Cryptography and network security: principles and practice*.

[14] The Korean Intellectual Property Office (2002) *A patent tendency of an information security technique*.

[15] Digital watermarking, <*http://www.ece.uvic.ca/~aupward/w/watermarking.htm*>

[16] Pour A.N., Kumekawa K., Kato T., Itoh Sh. (2007) *Elsevier: Computer Networks* 51, 4727-4743.

[17] Zhu S., Yao C, Liu D., Setia S., Jajodia S. (2007) Computer Communications 30, 793-806.

[18] Xiliang L., Eskicioglu AM. (2003) *Internet and Information Technology.*