A Selective Encryption/Decryption Method of Sensitive Music Usage History Information on Theme, Background and Signal Music Blockchain Network

Youngmo Kim, Byeongchan Park
and Seok-Yoon Kim*

Dept. of Computer Science and Engineering, Soongsil University, Korea, Republic of
E-mail: ymkim282@ssu.ac.kr; pbc866@gmail.com; ksy@ssu.ac.kr
**Corresponding Author*

Received 05 January 2022; Accepted 24 February 2022;
Publication 18 April 2022

Abstract

The theme, background, and signal music usage history information consists of general information such as music information, platform information, and music usage information, and sensitive information such as rights management information, music usage permission range, and contract information. If sensitive information among these is disclosed, disputes such as trade secrets and infringement of personal information protection between companies or between companies and individuals may arise.

We propose a selective encryption/decryption method to secure the confidentiality, integrity, reliability and non-repudiation of sensitive music usage history information used in the theme, background, and signal music blockchain environment. In the proposed method, a monitoring company encrypts sensitive information using a secret key for usage history information, which is combined with general information, and digitally signs it using

Journal of Web Engineering, Vol. 21_4, 1265–1282.
doi: 10.13052/jwe1540-9589.21411

a private key to register it in a block. A trust group can view and access the information at the time of inquiry by verifying the digital signature with the public key of the monitoring company and then can decrypt the sensitive information using the private key.

Keywords: Theme/background/signal music, monitoring, blockchain, encryption/decryption, music usage history.

1 Introduction

Recently, issues have arisen regarding the copyright protection and fair and transparent settlement and distribution of theme, background, and signal(hereinafter denoted as TBS) music [1–3]. In order to address these issues, transparent and reliable settlement and distribution should be made based on the acquition and disclosure of accurate usage information for TBS music [4].

Music usage information is music usage history information that a monitoring company creates by monitoring music used by broadcasters and personal broadcasting platforms. It consists of both contract information such as the scope and amount of permission for music use between the users, and sensitive information, which is the music owner's right management information. In particular, if sensitive information is disclosed, disputes such as trade secrets and infringement of personal information between companies or between companies and individuals may arise [5–7].

This paper proposes a method not only to secure the reliability and integrity of the information stored in the block [8–11] on TBS music blockchain network, but also to solve the non-repudiation problem by allowing the private key to be decrypted only with the trust company's private key. In the proposed method, the monitoring company encrypts the sensitive information based on a symmetric key using AES algorithm [12] so that only the sensitive information is selectively encrypted in the music usage history and only permitted parties can check it, and then generates music usage information using digital signature [13] based on an asymmetric key and stores it on a block. In order to view the generated information, the trust group can verify the digital signature with the public key of the monitoring company and decrypt the private key with the private key of the trust company to view the information [14, 15].

The structure of this paper is as follows. Following the Introduction, Section 2 briefly describes the method of generating music usage history information on blockchain network, the AES algorithm based on symmetric

key, and the digital signature used in the blockchain. Section 3 describes the proposed selective encryption/decryption method of music usage history information on the TBS music blockchain network. The verification of the proposed method is performed in Section 4, and the conclusion is given in Section 5.

2 Related Works

2.1 Music Usage History Information Generation Method in the Blockchain Network Environment

In the TBS blockchain network environment, a monitoring company monitors broadcasters and personal broadcasting platforms and generates music usage history information [5, 6]. The music usage history information generation method and block generation process are shown in Figure 1.

The music usage history information data format [5, 16] registered in the block is shown in Table 1.

In addition, such information as rights management information and contract information is required for the monitored information, and rights management information can be checked based on the UCI code. The music usage history information generated in this way is registered in the block and

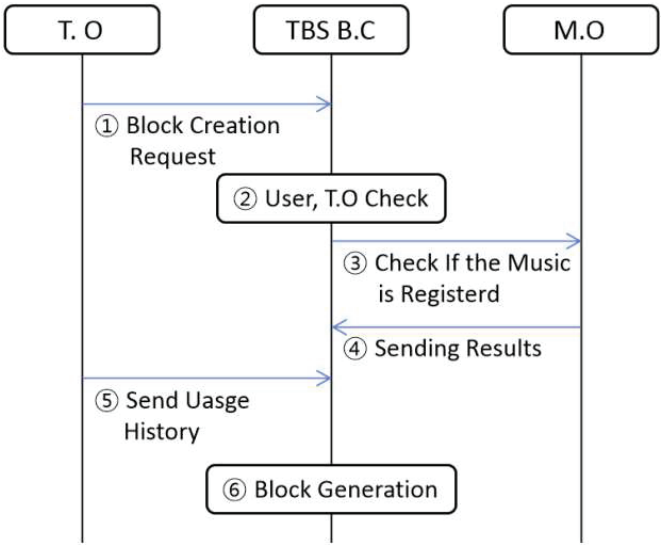

Figure 1 Block generation process on TBS music blockchain network.

Table 1 TBS music usage history information data format

Item	Explanation
Date	The date the content was played
Channel Code	Broadcaster channel code
Start Time(Pro)	Program start time
End Time(Pro)	Program end time
Program Title	Program title
Start Time(Music)	Music start time
Start Time(Music)	Music end time
UCI	UCI code

disclosed. However, there is a problem in that sensitive information such as company information is disclosed.

2.2 AES Algorithm

The AES (Advanced Encryption Standard) algorithm [12] is an algorithm created by the American Institute of Standards and Technology. It is a block encryption algorithm with a block size of 128 bits, and has the feature that various keys such as 128 bits, 192 bits, and 265 bits can be used. AES-128, AES-192, and AES-256 perform the same operation, but the key sizes and number of repetitions are different. The AES encryption algorithm is referred to as an algorithm of a Substitution Permutation Network (SPN) structure. It is a process of mixing rows and columns as one matrix with a structure that repeats substitution, as shown in Figure 2.

2.3 Digital Signature in Blockchain

Representative technologies of digital signatures include hash functions and asymmetric key encryption methods [13]. Since digital signature is a technology that can confirm whether data has been altered by encrypting it with a private key and decrypting it with a public key, the original can be maintained. It is one of the key aspects of ensuring the security and integrity of data recorded on the blockchain. When the sender sends data to the receiver, the sender encrypts the document with the sender's private key and sends it to the receiver.

Blockchain uses digital signatures to transmit transactions. The transaction details are encrypted and the public key paired with the private key used for signing is transmitted together with the signed transaction details. The recipient of this transaction opens the transaction content with the public key

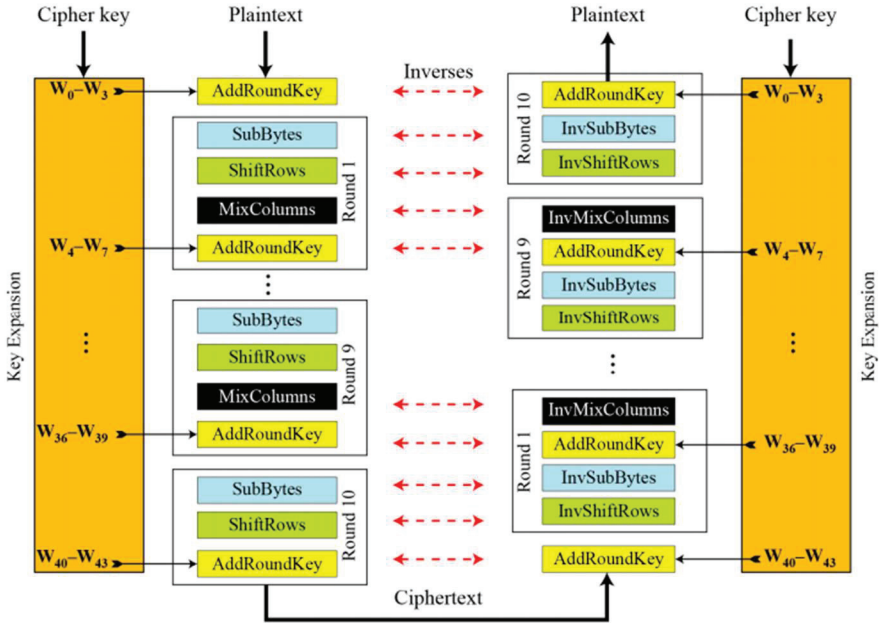

Figure 2 AES encryption/decryption process.

received along with the transaction content and compares it with the original transaction content. In comparison, if the contents of the two transactions are the same, you can be sure that the public key was sent by the owner. Digital signatures use asymmetric keys and hash functions in the blockchain to verify the authenticity of data in the following way. Since all transaction information contained in the block chain includes a digital signature, the transaction information can be trusted, and the process is shown in Figure 3.

3 A Selective Encryption/Decryption Method of Sensitive Music Usage History Information

3.1 An Encryption/Decryption Architecture for Music Usage History Information

The Stakeholders of music usage history information stored in the TBS music blockchain network consist of a monitoring company (MC), a trust organization (TO), a blockchain network, and an authentication server, the overall view of which is shown in Figure 4.

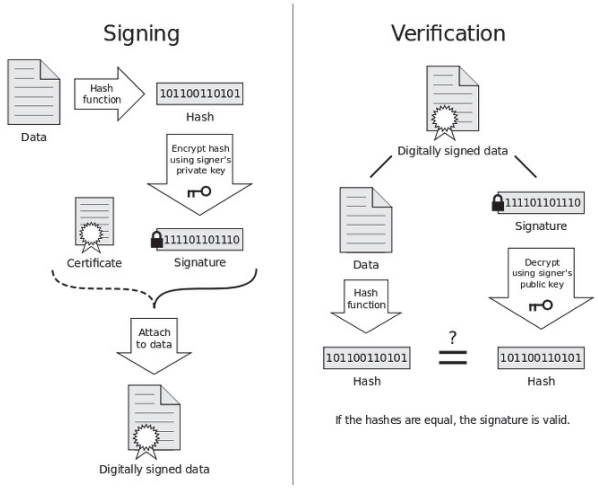

Figure 3 Digital signature in blockchain.

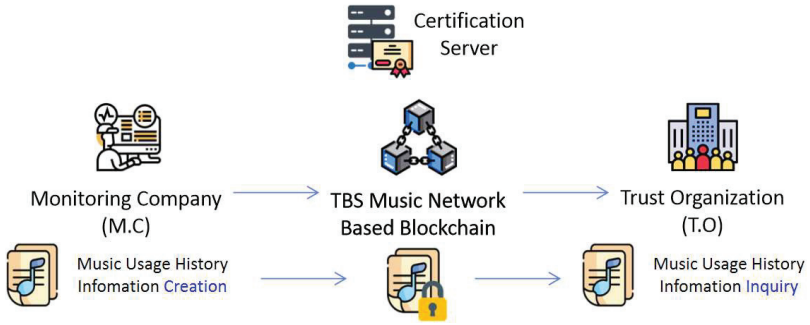

Figure 4 Stakeholders of music usage history information.

– TBS Music Blockchain Network

The TBS music blockchain network manages a number of monitoring companies and trust organizations based on a private blockchain, and enables the recording and sharing of music usage history information generated by the monitoring companies.

– Authentication Server

The authentication server generates the private key and public key of the monitoring company and trust organization so that it can be digitally signed with the private key, and the signed information can be verified with the public key. In addition, a secret key is generated to selectively encrypt/decrypt

Table 2 TBS music sensitive information

Category	Element	Subelement	Explanation
Music Info	Identifier	UCI Code	TBS music unique identifier provided by the Korea Copyright Commission
		ISRC	International standard record identifier
	Music Title	Title	Title representing TBS music
		Subtitle	TBS music subtitle
	Album	Album Code	Unique identifier to identify the album
		Album Title	Title representing the album
		Album Subtitle	Subtitle of the album
Usage Info	Biz Man	Biz Man Code	Music user identification code
		Biz Man Name	Name of the music operator
	Service	Content Name	Content name in which music is used
		Media Dlassification	Service media used by music users
	Music Usage Info	UCI	TBS music unique identifier provided by the Korea Copyright Commission
		Title	Title representing TBS music
		Use Time	Time the music was used during main delivery in the content
		Usage Section	The section in which music is used in the entire length of the content

the sensitive information. It is assumed that the key is transmitted securely in all processes of generating and transmitting the key.

– Monitoring Company

The sound source usage history information generated by the monitoring business is divided into general information and sensitive information. Sensitive information is shown in Table 2 and general information is shown in Table 3.

Among them, sensitive information is encrypted with a secret key. Then, it is digitally signed together with general information and registered in the block on TBS music blockchain network.

Table 3 TBS music general information

Category	Element	Subelement	Explanation
Rights Info	Copyright Holder	Copyright Holder Code	Unique identifier of the copyright holder/organization of TBS music
		Copyright Holder Name	People/organizations that own the copyright of TBS music
		Copyright Holder Role	Role that owns the copyright of TBS music
		Ownership Info	Share of TBS Music
	Contract Contents	License Range	In the case of a music license agreement, the scope of license in the agreement
		Rights Type	Classification of rights to works prescribed by law
Management Info	Biz Man	Biz Man Code	Unique identifier code for each music service provider
		Biz Man Name	Music service company name
	Settlement Code		Settlement code according to service type of music service company
	Music Code		Music service company's music management code
Settlement Info	Price	Revenue Info	Revenue information such as usage fees incurred by the service
		Settlement Cost	The rate that the service provider pays the right holder

– Trust Organization

The trust group receives the music usage history information registered in the block, verifies the signature, and decrypts the sensitive information with the private key to view the usage history information.

3.2 A Selective Encryption/Decryption Method of Sensitive Information in Music Usage History

The selective encryption/decryption method of sensitive information in music usage history proposed in this paper is divided into three processes: first, key generation and delivery process, second, optional encryption and block registration process, and finally, the process of reading, decrypting, and

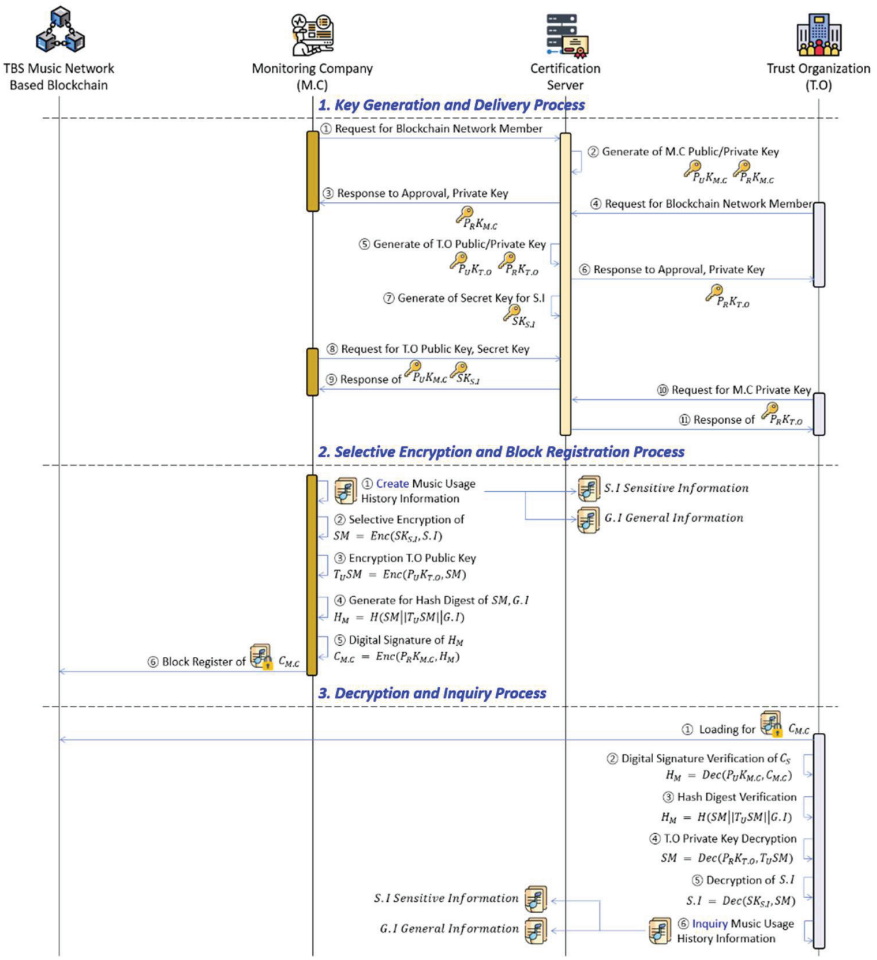

Figure 5 Overall selective encryption/decryption process of music usage history information and digital signature process.

retrieving the information from a block. The overall process is illustrated in Figure 5.

First, the key generation and delivery process involves the digital signature/verification of the monitoring company, the public key that can be encrypted/decrypted so that only trust organizations can read it, and the private key generation and the private key to selectively encrypt sensitive information on music usage history The generation process and key delivery process are shown in Figure 6.

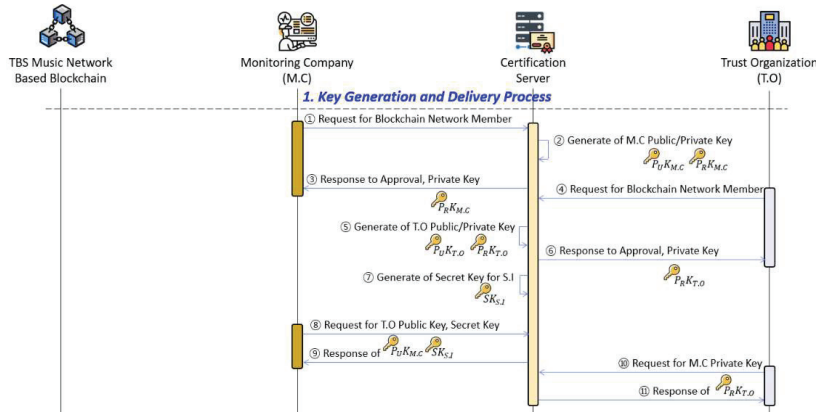

Figure 6 Key generation and delivery process.

The monitoring company makes a request to the authentication server to participate in the TBS blockchain network. The authentication server creates with the monitoring company's public key($P_UK_{M.C}$) and private key($P_RK_{M.C}$). The authentication server delivers the generated private key to the monitoring company and stores the public key. The trust organization makes a request to the authentication server to participate in the TBS blockchain network. The authentication server generates a public key($P_UK_{T.O}$) and a private key($P_RK_{T.O}$) of the trust organization. The authentication server delivers the generated private key to the trust organization and stores the public key. The authentication server generates a secret key($SK_{S.I}$) for the selective encryption/decryption of sensitive information in music usage history generated by the monitoring company. The monitoring company requests the trust organization's private key so that only the trust organization can decrypt and selectively encrypt the sensitive information in the generated music usage history information. The authentication server transmits the public and private keys of the trust organization. The trustee requests the public key of the monitoring company to verify the digital signature. The authentication server transmits the public key of the monitoring company.

Secondly, the selective encryption and block registration process selectively encrypts only the sensitive part among the music usage history information generated by the monitoring company using the private key, encrypts it with the trust group private key so that only the trust group can read it, and digitally signs with the monitoring company's private key and registers the block, as shown in Figure 7.

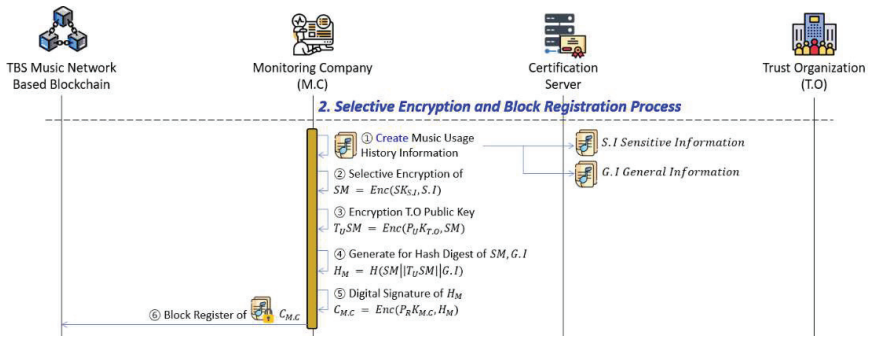

Figure 7 Selective encryption and block registration process.

Monitoring company monitors broadcasting companies and creates music usage history $G.I$ (general information) and $S.I$ (sensitive information). Among them, SM (Selective Message) is generated after selectively encrypting ***S.I*** using $SK_{S.I}$ (secret key). The generated SM is encrypted using $P_UK_{T.O}$ (the public key of the trust organization) so that only the trust group can read it, and then T_USM is created. Then, SM, T_USM and $G.I$ are concatenated for digital signature and hash digest is generated. Before it is registered in the generated block, it is signed with the private key of the monitoring company, $P_RK_{M.C}$, and then $C_{M.C}$ is created and registered in the block by the monitoring company.

$$\begin{aligned} SM &= Enc(SK_{S.I},\ S.I) \\ T_USM &= Enc(P_UK_{T.O},\ SM) \\ H_M &= H(SM||T_USM||G.I) \\ C_{M.C} &= Enc(P_UK_{M.C}H_M) \\ &= S.I||T_USM||H_M||G.I \end{aligned}$$

Finally, the decryption and inquiry process is the process in which the trust organization retrieves, decrypts, and inquires the general and sensitive information of the signed sound source usage history registered in the block, as shown in Figure 8.

The trust group calls $C_{M.C}$ registered in the block, verifies the signature using $P_UK_{M.C}$(the public key of the monitoring company), and extracts H_M. The extracted H_M is a hash value in which SM, T_USM, $G.I$ are concatenated, and it is decrypted through $P_RK_{T.O}$ (private key of trust

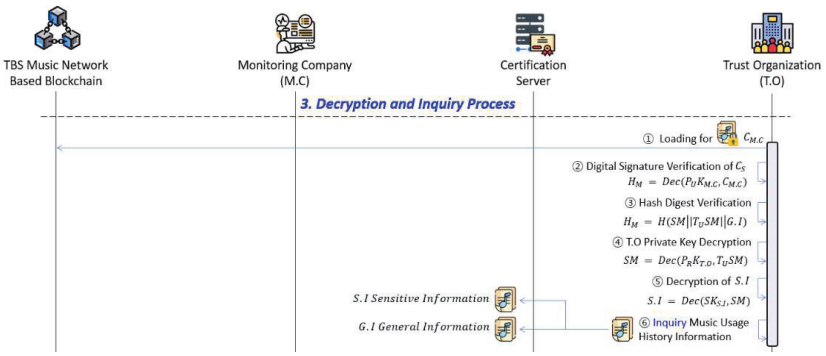

Figure 8 Decryption and inquiry process.

organization) and $SK_{S.I}$ (secret key), respectively, so that $S.I$ can be finally searched, and $G.I$ can also be searched.

$$\begin{aligned} H_M &= Enc(P_U K_{M.C},\ C_{M.C}) \\ &= H(SM||T_U SM||G.I) \\ SM &= Dec(P_R K_{T.O},\ T_U SM) \\ S.I &= Dec(SK_{S.I},\ SM) \end{aligned}$$

4 Security Assessment

4.1 Confidentiality of Information

Music usage information stored or shared in a block on TBS blockchain network must be confidential to protect the content of the information to prevent third parties from accessing or modifying the information. In the method proposed in this paper, when a monitoring company selectively encrypts only sensitive information during music usage information generation process, it encrypts it with a secret key and additionally encrypts it with a trust organization's private key, which guarantees that only the trust organization can view the usage history.

– Secret key based $S.I$ encryption/decryption

$$\begin{aligned} SM &= Enc(SK_{S.I},\ S.I) \\ S.I &= Dec(SK_{S.I},\ SM) \end{aligned}$$

– Trust organization public key based private key encryption

$$T_U SM = Enc(P_U K_{T.O},\ SM)$$
$$SM = Dec(P_R K_{T.O}, T_U SM)$$

4.2 Integrity of Information

Integrity must be ensured to ensure that the information prototype has not been tampered with. The method proposed in this paper can guarantee integrity because it is virtually impossible to forge or falsify once it is recorded due to the nature of the blockchain technology. In addition, in the process of decrypting $C_{M.C}$, it is possible to check its integrity by comparing it with $S.I$.

$$Certificate = P_U K_{M.C}$$
$$H'_M = Dec(P_U K_{M.C},\ C_{M.C})$$
$$= H(SM||T_U SM||G.I)$$
$$Compare,\ H_M =?\ H'_M$$

4.3 Reliability of Information

When the information is created and registered in the block, it is digitally signed based on the monitoring company's private key, so if the signature can be verified, it is regarded as not being changed. Since only signed music usage history information is registered in the block, the reliability of the information is guaranteed. In addition, since $S.I$ is encrypted before being signed, the reliability of information can be secured because it is encrypted with the private key of the trust organization that reads the information.

– Public key-based digital signature of the monitoring company

$$H_M = H(SM||T_U SM||G.I)$$
$$C_{M.C} = Enc(P_U K_{M.C} H_M)$$
$$= S.I||T_U SM||H_M||G.I$$

– Signature verification

$$H_M = Dec(P_U K_{M.C},\ C_{M.C})$$

4.4 Non-repudiation of Information

The private key is encrypted with the public key of the trust organization so that the information generated by the monitoring company can be viewed only by the trust organization. Then, since the private key of the trust organization can be decrypted and viewed, only the trust organization can actually see it, which means the non-repudiation in the case of information leakage.

– Encryption/decryption based on private key of trust organization

$$T_U SM = Enc(P_U K_{T.O}, SM)$$
$$SM = Dec(P_R K_{T.O},\ T_U SM)$$

5 Conclusion

In this paper, we proposed a method of selectively encrypting/decrypting the sensitive information in sound source usage history generated by monitoring companies. Since music usage history information contains general information and sensitive information that should not be disclosed, selective encryption/decryption of sensitive information is used to prevent leakage of corporate information that may occur when registering or inquiring music usage history information on the blockchain network. When the proposed method is used, the sensitive information such as rights management information, music usage permission range, and contract information stored in the block chain are securely encrypted. It provides the advantages of securing the confidentiality of information, the reliability of the information producing party, non-repudiation, and the integrity of the information stored in the ledger. In addition, the sound source usage history information generated in this way can be used as raw data for the fee settlement and distribution process. As a future study, it is necessary to apply the proposed model to the actual system and to investigate the various exception handling that may occur when the system is operated.

Acknowledgement

This research project supported by Ministry of Culture, Sport and Tourism (MCST) and Korea Copyright Commission in 2020 (2020-MC-9400).

References

[1] E. S. Hwang, "Have you ever heard the word 'TBS'," *Chosunpub*, 2016.
[2] B. G. Kim, "Suggestions for creating a sustainable K-pop industry ecosystem," KOFICE, May, 2019.
[3] H. G. Kim, "It's noisy when money comes in for beautiful music," *Sisa Journal*, Vol. 931, 2015.
[4] K. Y. Bang, K. B. Nam, K, Y. Jung and K. S. Han "A Study of Music Copyrights System by the Monitoring of Music on Broadcasting (Fingerpring Technology Centrally)," Journal of The Korea Society of Information Technology Policy & Management, Vol. 7, No. 3, pp. 13–17, 2015.
[5] Y. M. Kim, B. C. Park, K. S. Bang and S. Y. Kim, "A Method of Generating Theme, Background and Signal Music Usage Monitoring Information Based on Blockchain," Journal of The Korea Society of Computer and Information, Vol. 26, No. 2, pp. 45–52, 2021.
[6] Y. M. Kim, B. C. Park, S. Y. Jang and S. Y. Kim, "A Method of Generating Theme, Background and Signal Music Usage Monitoring Information Based on Blockchain," Journal of Semiconductor & Display Technology, Vol. 20, No. 1, 2021.
[7] S. H. Han, "[Friendly IP] "Who has ownership of works that are suitable for external parties?"," BIZ WORLD, 2020.
[8] K. N. Lee and G. H. Jeon, "A Study on Improvement of Used-goods Market Platform Using Blockchain," Journal of Digital Convergence, Vol. 16, No. 9, pp. 133–145, 2018.
[9] J. S. Park and S. U. Shin, "Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection," Journal of Internet Computing and Services, Vol. 20, No. 6, pp. 105–117, 2019.
[10] E. Androulaki, C. Cachin, C. Ferris, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi and C. Stathakopoulou, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," EuroSys '18: Proceedings of the Thirteenth EuroSys Conference, No. 30, pp. 1–15, 2018.
[11] I. D. Yoo, W. S. Lee, H. J. Kim, S. Y. Jin and S. H. Jo "Blockchain Technology and Utilization Schemes in Tactical Communication Network," Journal of The Korea Society of Computer and Information, Vol. 23, No. 12, pp. 49–55, 2018.

[12] Hua Li, Jianzhou Li, "A new compact dual-core architecture for AES encryption and decryption," Electrical and Computer Engineering, Canadian Journal of Vol. 33, pp. 209–213, 2008.
[13] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm(ECDSA)," International Journal of Information Security, Vol. 1, No. 1, pp. 36–63, 2001.
[14] Y. A. Min and Y. T. Baek "A Study on the Application of Block Chain Ethereum Technology to Activate Digital Contents Trading as Sharing economy – data encryption and modify merkle tree-," Journal of The Korea Society of Computer and Information, Vol. 23, No. 10, pp. 73–80, 2018.
[15] E. G. Jang, "User Authentication Technology Using Multi-Blocks in the Cloud Computing Environment," Journal of the Korea Society of Computer and Information, Vol. 25, No. 11, pp. 139–146, 2020.
[16] TTAK.OT-10.0334, "Metadata Elements of Copyright Transfer Information on Digital Music Contents," 2012.

Biographies

Youngmo Kim received his Ph.D degree in Computer Engineering from Deajeon University, Daejeon Korea in 2011. He is currently adjunct professor in Soongsil University. He is also working on several standardization and national project.

Byeongchan Park received the B.S., M.S., dgree in Computer Science and Engineering from Soongsil Unversity, Korea, in 2015 and 2018, respectively. He is Currently a Ph.D Student in the Department of Coumputer Science and Engineering, Soongsil University.

Seok-Yoon Kim received the B.S degree in electical engineering from Seoul National University in 1980. He received the M.S and Ph.D degree in ECE from University of Taxas at Austin, in 1990 and 1993, respectively. He is currently a Professor in the School of Computer Science and Engineering, Soongsil University.