- ORIGINAL ARTICLE -

Blockchain-Based Music Wallet for Copyright Protection in Audio Files

Billetera De Música Basada En Blockchain Para Protección De Derechos De Autor En Archivos De Audio

Remzi GÜRFİDAN[1], Mevlüt ERSOY[2]

[1]*Isparta University of Applied Science, Yalvac Technical Sciences Vocational School, Turkey*
remzigurfidan@isparta.edu.tr
[2]Süleyman Demirel University, Computer Engineering, Turkey
mevlutersoy@sdu.edu.tr

Abstract

The works produced within the music industry are presented to their listeners on a digital platform, taking advantage of technology. The problems of the past, such as pirated cassettes and CDs, have left their place to the problem of copyright protection on digital platforms today. Block chain is one of the most reliable and preferred technology in recent times regarding data integrity and data security. In this study, a blockchain-based music wallet model is proposed for safe and legal listening of audio files. The user's selected audio files are converted into block chain structure using different techniques and algorithms and are kept securely in the user's music wallet. In the study, performance comparisons are made with the proposed model application in terms of the length of time an ordinary audio player can add new audio files to the list and the response times of the user. The findings suggest that the proposed model implementation has acceptable differences in performance with an ordinary audio player.

Keywords: Blockchain, Music Wallet, Copyright Protection, Data Security

Resumen

Las obras producidas dentro de la industria de la música se presentan a sus oyentes en una plataforma digital, aprovechando la tecnología. Los problemas del pasado, como los casetes y CD pirateados, han dejado su lugar al problema de la protección de los derechos de autor en las plataformas digitales de hoy. Blockchain es una de las tecnologías más confiables y preferidas en los últimos tiempos en lo que respecta a la integridad y seguridad de los datos. En este estudio, se propone un modelo de billetera de música basado en blockchain para escuchar archivos de audio de manera segura y legal. Los archivos de audio seleccionados por el usuario se convierten en una estructura de cadena de bloques utilizando diferentes técnicas y algoritmos y se guardan de forma segura en la billetera de música del usuario. En el estudio, se realizan comparaciones de rendimiento con la aplicación modelo propuesta en términos de la cantidad de tiempo que un reproductor de audio normal puede agregar nuevos archivos de audio a la lista y los tiempos de respuesta del usuario. Los hallazgos sugieren que la implementación del modelo propuesto tiene diferencias aceptables en el rendimiento con un reproductor de audio común.

Palabras claves: Blockchain, Music Wallet, Protección de derechos de autor, Seguridad de datos

1. Introduction

Music composed and interpreted by musicians has become a form of record, cassette, cd, dvd, adapting to technological innovations over time to meet the listeners. Today, music meets its listeners mostly in digital music form. It is known that all artists and producers who worked in the music industry before the rise of the trend towards digital music suffered considerable financial damage from illegal commercial activities such as pirated cassettes and pirated CDs. This situation has left its place to the problem of protecting the copyright of the work produced on the digital platform of music.

The digital watermark method has been preferred to secure audio files on digital platforms in studies and recommended models. In the works, audio files are fragmented and digital watermarks are embedded in peak points, ensuring the security of audio files. Although different watermark methods based on Fourier transforms are preferred in different studies on similar subjects, the general protection principle is the same [1, 2]. In another mathematical model-weighted study [3] a flexible voice ownership protection scheme was proposed to improve security

by integrating discrete Wavelet Transform and discrete Cosine Transform into visual cryptography and digital time stamps. According to the experimental results, the proposed model fulfils several characteristics of property protection, including perceptual transparency, blindness, robustness, security and openness [3]. The preferred digital watermark method can be permanently embedded in the audio file as well as erasable forms are available [4]. Another alternative study proposed a method for preserving audio files that combines reduced difference expansion with generalized difference expansion methods [5].

With the popularization of the concept of digital data, different technical programs and attack strategies are being developed for the capture of this data by cyber attackers. To prevent these threats, many technologies, especially in the cybersecurity field, have stepped up their work on data security. Blockchain technology welcomes us as a new technology that can solve exactly this situation and deliver reliable results due to its basic structure. The basic principle of Blockchain operation is that before the new chain ring is added, the data to be added is associated with the previous records and added to the chain. In Blockchain technology, when a transaction is approved and added to the chain, it becomes impossible to change and thus becomes tamper-resistant [6]. Blockchain is the preferred method of protecting data on different features held on digital platforms [7-9].

In this study, a practice was developed to protect the labor of producers and musicians who work in the music industry and produce products. The developed app offers its users a personal music wallet. The user adds the music to the music wallet from which he / she has the rights to listen. With the realization of this process, the music acquired is stored in the wallet in a secure and tamper-free manner, subject to different algorithms. The security of the music wallet and the security of the copyrights of the music in it are provided by blockchain structure.

The contributions and innovations of the proposed model to the literature are as follows.

- A model has been developed using the blockchain structure so that music files can be listened to securely.

- AES128 bit encryption algorithm is used to encrypt audio files in Blockchain chains.

- For data protection every decoded chain block is stored only on RAM, and the decoded file on RAM is played directly without any HDD usage.

- Each music file in the wallet is stored with Dynamic Encryption connected to each other using public and private keys to improve strength of blockchain.

2. Literature Survey

In the areas of ensuring data security and protecting data integrity, scientists have applied different methods such as cloud computing [10-12], distributed data storage security [13], cryptography [14,15]. Block chain technology, which has been introduced into the literature in recent years, is frequently preferred in the field of data security and data integrity, and appears in many academic studies. In their work, scientists use block chain technology both for the integrity and security of raw data [16-19] and for the realization of commercial activities of individuals and businesses with smart contracts [20.21]. In this study, block chain technology was used to ensure the integrity and security of audio files. Different scientists have done previous studies to preserve sound files.

In their study, Shelke and Nemade used watermark, a method of hiding information signal into digital form based on spread spectrum, to protect the copyright of audio files. They have created watermarks that break down audio and video files and embed them in different parts. Thus, the file with watermark has become whole. Copying and verification of files can be controlled by Watermark [22]. Similar to this study, Xu and his colleagues propose a new multi-watermark scheme that places three watermarks that serve different purposes in the same digital audio file. Robust watermark performs copyright protection function because it is resistant to various signal attacks. The semi-brittle watermark is robust against common signaling operations. The fragile watermark is sensitive to any small change in the audio signal, so it has been used to verify data integrity [23].

In enterprise resource planning (ERP) systems requiring special hardware and software security, Hrischev proposed a new database model based on the blockchain structure. He described his proposed model as more secure, more transparent and the organizational model of the future in ERP systems [24]. Kumar and Tripathi hid patient data using blockchain infrastructure on the Health Network, where data privacy is vitally important. They have preferred smart contracts to secure data on the network. They used the Linux-supported Hyperledger Fabric and Hyperledger composer modeling tool to build the Blockchain structure [25].

Blockchain technology has also started to be used in works on copyright protection. In their study, Meng and colleagues proposed a blockchain-based copyright management model using digital watermark. In their proposed model, they install and decode blockchains using QR codes and encryption algorithms by applying the digital watermark on image files. They plan to try this method on audio and video files in their future work [26].

In their work, Zhao and O'mahony have implemented an Ethereum application based on

Blockchain and intelligent contract technology to protect music copyright and secure rights holders ' revenues. They planned to use two bands, a musician and a Fan band. The musician loads the file into the system. The loaded file is signed with a digital signature. It is encrypted with the AES algorithm. The Fan group can select the audio file they want and listen to the music they bought after making their payment on the Ethereum platform. The fact that the artist's income cannot be hidden in the application is undesirable [27]. In our proposed model, audio files are not signed using a digital watermark. We used our preference for AES 128-bit encryption. The binary form, chain form and hash form of the audio files are kept in separate columns in the database where the audio files are kept in the music wallet. The password used to encrypt the music included in the music wallet is kept in a blockchain structure and is dynamically generated from the hash form of different columns.

Lee, K. S. and who, S. K. They have made a proposal to protect audio files with blockchain technology. Their work is based on the principle of signing audio files with the sound signature they obtained from that file. The 20-byte hash value of the generated audio signature and audio source file is added to the block process data and included in the blockchain. However, in this study, the proposed method was mainly studied with a focus on block size (scalability), and efficiency aspects such as the time and cost required were not taken into account. Accordingly, an experiment should be conducted on certain conditions by applying a real system as Post-Research [28].

3. Proposed Model

There are various methods and processes in developing the proposed model in the study. These methods and processes are described in detail in Table 1.

In this study, a blockchain-based music wallet application was developed in order to protect the copyrights of works produced in the music industry. The aim of the study is to reach who do not have the right to listen to music works which are guaranteed safety by using this application. it is to make it inaccessible by people.

In the database to be used for music wallet, the sound file id, musician name, name of the sound file, album name, encrypted version of the sound file, key block chain used for encryption and hash form of the sound file are kept. In order to create database records, the tags of the audio file to be uploaded by the owner of the music wallet must be read. TagLibSharp library was used to perform this process. In order not to keep the music file raw in the database, the SHA256 extract form was calculated.

For Hash operation, the audio file is read primarily as a byte array and transferred onto RAM. The SHA256 hash form of the Byte array is calculated. The resulting hash is saved in the nvarchar(max) data type to the database using the Base64 encoding method to read the form again. The Base64 encoding method is a technique for converting binary data into text format. Data in Binary form consists of 8-bit byte sets. For the Base64 form, this 8-bit data is divided into 6-bit parts. This is because 64 different numbers expressed in 6 bits are paired with 64 different characters in the ASCII character set. Base64 Encoding is done when the 6-bit divided data is matched to its equivalent in the ASCII table. The proposed model is shown in Figure 1.

Table 1 Functions and features used in the proposed model

Symbol	***Abbreviation***	***Function***
M_i	Audio Files	Raw audio files
W_i	Audio Wallet	Secure audio store where music is kept
RAF	ReadAudioFile	Function of reading audio files
S	Source	Raw audio source
LC	LastChain	Get last chain data function
T	Tag Array	Array in which the audio file tags are kept
SAT	SplitAudioTags	Separating audio file tags function
PK	PrivateKey	Personal Private Key
TRS	TagRemaining Skip	Tag remaining skip function
GUF	GetUTF8Form	Get UTF8 form function
NCA	NewChainAdd	Add new row to blockchain
GH	GetHash	Get Hash form function
CB	ConvertBase64	Convert to Base64 form function
WD	WriteDatabase	Write database function
H	Hash	Hash
E	Encrypted	Data block of encrypt with AES
GB (Array,n)	Getbyte	Get nth byte of array function
IV	Iteration Vector	AES algorithm use IV for encryption process
EA	EncyrptAes	AES encryption function
DA	DecyrptAes	AES decryption function
M_i^c	Encrypted Audio File	Encrypted Audio File

In Figure 1, the operation of the model is schematized into four main modules and the relationships between them are shown.

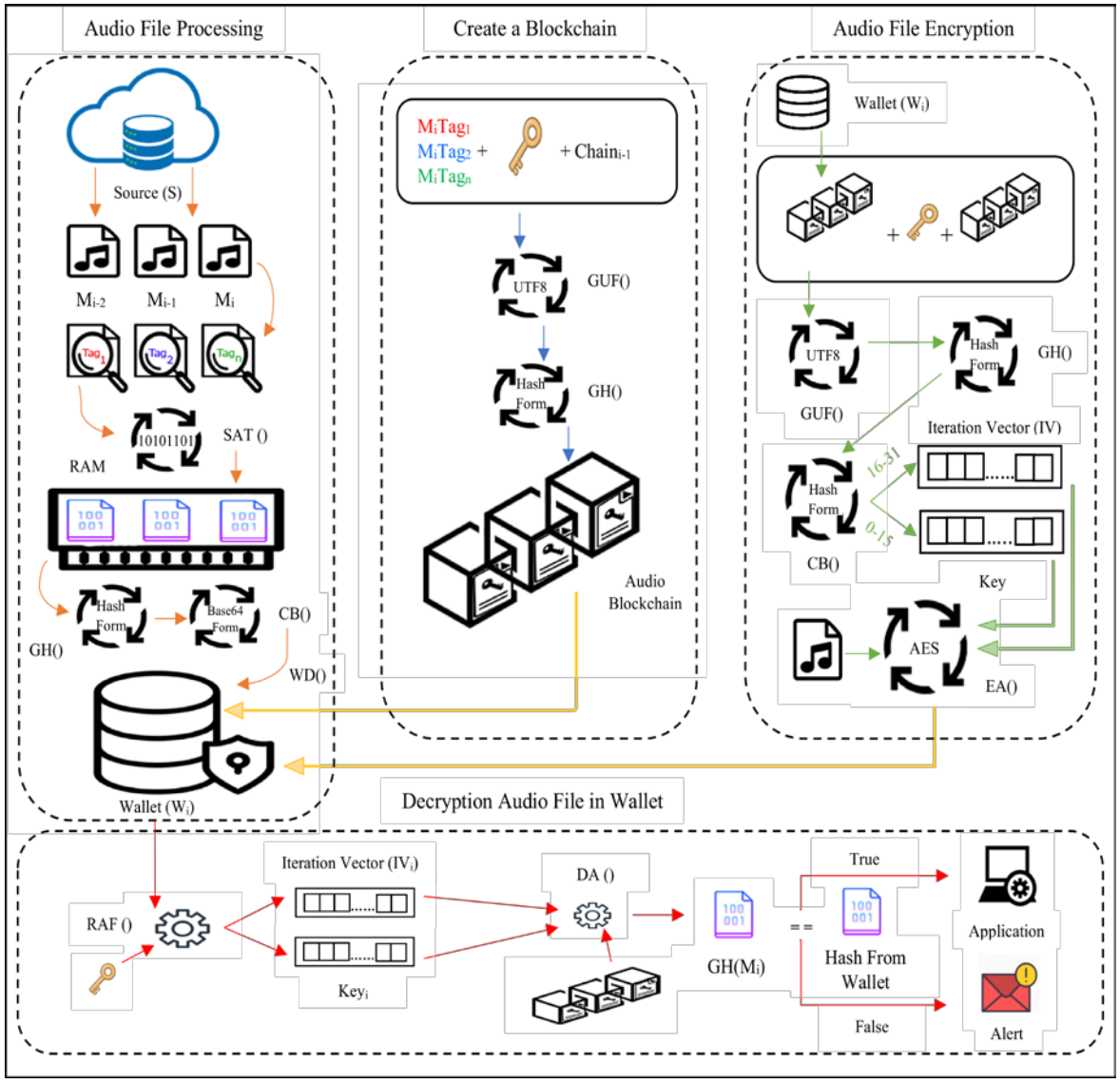

Fig. 1 Proposed model architecture.

3.1. Create Blockchain

In the process of creating the block chain, different operations were performed for the first entry to insert. The album name, audio file hash, audio file name, musician name and personal private key, which are read primarily from file tags, are combined in sequence as strings. The bytes of the value generated by the UTF8 encoding method are taken. It is then added to the end of the chain as a new ring, which is extracted using SHA256 algorithm. This last chain value is written to the databas. The new block chain ring is calculated with the model shown in Eq (1).

$$LC_i = T_i + \sum_{i=0}^{i\,!=null} M_i + PK + LC_{i-1} \qquad (Eq.1)$$

Similar operations have been performed for the subsequent records that will occur during the creation of the blockchain. The album name, audio file extract, audio file name, musician name, chain data of the previous record, and user Key are combined with the sequence as string. The bytes of the value generated by the UTF8 encoding method are taken. It is then added to the end of the chain as a new ring, which is extracted from the extract using SHA256. This last chain value is written to the database.

Algorithm 1 Creating an audio blockchain

Input: Album name, Audio file hash, Audio file name, Performers name, Previous chain, Personal private key

Output: New chain member

1: M_i = RAF(S)
2: **foreach** (Mi.Tags>0)
3: T[i] += SAT(Mi)
4: TRS ()
5: T[i] += PK + $Chain_{i-1}$
6: Byte [] $Value_i$ =GUF(T[i])
7: $Chain_i$ = NCA ($GH(Value_i)$)
8: WD(CB($Chain_i$))

3.2. Encrypt Audio File

The fact that the files in the music wallet are in raw form in the database will bring possible security weaknesses. For this reason, it is preferred to keep the files in encrypted format in the database.

Different operations were carried out for the first music file to be recorded in the database. Firstly, the block chain and the personal private key were added to the music file. Then, the bytes of the form UTF8 were taken and the hash was calculated with SHA256 algorithm. Then it is encrypted with AES 128-bit encryption algorithm, using the first 16 bytes as key, and the second 16 bytes as iteration vector as shown in Figure 2. Starting from the first recording (Mi) to the last recording (t_{max}), the encryption process shown in Eq (2) was repeated for each recording.

$$\sum_{i=0}^{t_{max}} EA(M_i, Key_i, IV_i) \qquad (Eq.\ 2)$$

Similar operations were performed for subsequent music files to be recorded in the database. First, the value of the last ring of the block chain and the user Key are added to the music file. Then, the bytes of the form UTF8 were taken and the essence was calculated with SHA256 algorithm. Then it is encrypted with AES 128-bit encryption algorithm, using the first 16 bytes as key, and the second 16 bytes as iteration vector as shown in Figure 2. The encryption key used in the AES encryption algorithm is calculated according to Eq (3) and provides a dynamic encryption system thanks to this mathematical model.

$$\sum_{i=0}^{t_{max}} GB(H_i, i) \qquad (Eq.3)$$

Algorithm 2 Encryption of audio files

Input: Audio blockchain, User key, Audio file
Output: Encrypted secure audio files, Audio file hash

1: M_i = RAF(S)
2: LC_i = LC (W_i)
3: $E_i = M_i + LC_i + PK$
4: Byte [] $Value_i$ =GUF(E_i)
5: H_i = GH($Value_i$)
6: **for** i=0 to i=15
7: Key_i +=GB(H_i,i)
8: **for** i=16 to i=31
9: IV_i +=GB(H_i,i)
10: EA (M_i, Key_i, IV_i)

3.3. Reading Files from Music Wallet

The music wallet checks the integrity (non-tamper ability) of the data in the database by using the saved key as soon as it starts operating. Starting from the First Ring of the chain formed, the control process confirms the essence created during the recording by comparing the reacquainted essence for that line and the recorded essence.

When the user is asked to read a file from the music wallet, the password and iteration vector used in encrypting the file, which were previously created using the blockchain and user Key, are recalculated. This value for each audio file is stored in a different column in the database, so the amount of data in the wallet increases, but it will not cause performance loss. The decoded version of the file is stored in a memory stream on RAM and played with the Naudio library. However, there is a significant vulnerability in the process. This weakness is the possibility that a different file encrypted with the same password can be changed in the database. To eliminate this situation, after decrypting the audio file, the SHA256 extract is calculated again just before playing the audio file and this value is compared to the value stored in the database. This allows you to ensure that the audio file is not tampered with in any way.

4. Findings and Discussion

Figure 3 shows how the sound files recorded in the wallet are stored in the study. The singers ' names were recorded in the "$Performers_i$" format so as not to cause any copyright problems. As shown in Figure 3, the name of the audio file, the singer and the album name are kept as raw data. In contrast, the audio file is kept in binary and hash forms. In addition to this data, the block chain is stored as a separate data column in the wallet.

The interface developed for listening to the audio files in the music wallet is shown in Figure 4, which is simple to use and decipherable. The created Dec. music wallet contains a list of audio files, add new audio files, play audio files, stop and skip buttons. In the study, we analyzed the performance Times of the proposed model and the developed application with an ordinary audio file player. In this analysis, we measured the time it takes for audio files to respond to user responses. We did this measurement with an object that we placed at the beginning and end of the code that we wrote and produced from the Stopwatch class. Intel i7 processor 2.60 Ghz, 16 GB of RAM and 500 GB of SSD hardware. The performance measurements obtained are shown in Table 2.

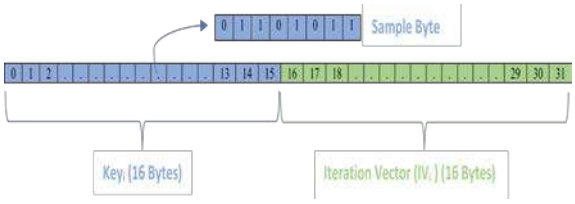

Fig. 2 AES Crypto Algorithm Parameters.

Performers	Audio_File_...	Album	Audio_File	Chain	Hash
Performers1	Kurban Oldu	Kararsızım	<Binary data>	pUYo8njCcIW38eQn+N7kFTSwVSh6jC6hmm6UB+4hmeg=	HdEmeGFY8ucUpP6k8RSYfMFplazfb6j5U8SaRYmsQe0=
Performers1	Kurban Oldu	Kararsızım	<Binary data>	q26pcBLSEiP+gSGfiPBgSxssZXoaU3d/+BbP+OV8JEo=	HdEmeGFY8ucUpP6k8RSYfMFplazfb6j5U8SaRYmsQe0=
Performers2	Dut Ağacı	Oyun Havaları	<Binary data>	0Z6Z65qRp6eblOm/ypk5R9aQf3N43/tgFBEscVbDK5Y=	ZHjyOVa+/Vk4qQdhiZ8Ghgk6mfHclwJAiO2UtR51I08=
Performers3	A Kuzum	Bağlama Orkestrası	<Binary data>	TVT2CqZeT/YSlow1D7I2fX3WG3TAXfa+tJzvu+MYR5k=	QAZWG1vJ+i3sGLOiz8I8TIBPj2bMXdA6nnwDHLMiUlc=
Performers4	Atim Arap	Camci Cam Nerede	<Binary data>	BsvpFkJiQn3V+OEw9eqccHvP7hgtAHUtxrhk1FHJKtI=	pyPW8ZYkfjkcWFAc+EYnIlerJUMhU7rPY+oWELLtGEU=
Performers5	Kazma	Sonkalp Nerede Kaldı	<Binary data>	EjivbxWL+qBOjtP0uOp2E6V6/mDnDHNdc1xJJLaKbKY=	bNFXg+zqjX/zazqtzFgx6gXu2JSmr3SxRVY3VHwoBfY=
Performers6	Gelme	Nerede Bilemiyorum	<Binary data>	4Cx8maSmSy6csw4/RPvq+2xFIFKEz9P68URb1qTaeP0=	jSO1AxlrcAE8H+2sVNaW7WAm+2EGW5ZUVv/CiNYy180=
Performers6	Hadi	Sevda	<Binary data>	6YpKFyFYFLDhMBLRdkQGQoFQiWv5hpKOWwapZKaRMPA=	mfPlo6eB+JxDYYqFlylE1uFpvIImPrHKs0KOLNp2Ga4=
Performers7	Bitsin Bu	Ah Bu Şarkılarda Olmasa	<Binary data>	m0c4VO4a7DFs6sjSyzZdUBQfg4/kmVTEto/6Vx03/1E=	r8yv/W7Jrckp0l/OJ5hhBjiK3IfkCxErMrQEEbtXq3Q=
Performers1	Oldu	Kararsızım	<Binary data>	0DiiDzeQOhSm/zNFLmrr+/7pGKGEpPZQ/dgI4L0elmw=	HdEmeGFY8ucUpP6k8RSYfMFplazfb6j5U8SaRYmsQe0=

Fig. 3 Data held in music wallet.

Table 2 Performance analysis of ordinary audio player with proposed model application

	Ordinary Audio File Player		*Recommended Model Application*	
Number of Audio Files in List / Wallet	***Adding Audio File to the List (sec)***	***Response to Command to Play Audio File (sec)***	***Adding Audio File to the Wallet (sec)***	***Response to Command to Play Audio File (sec)***
1	0.852	1.263	1.092	1.431
10	0.822	1.331	1.087	1.555
30	0.798	1.250	1.090	1.496
75	0.842	1.333	1.107	1.570
100	0.882	1.458	1.249	1.592

Fig. 4 Application that plays audio files

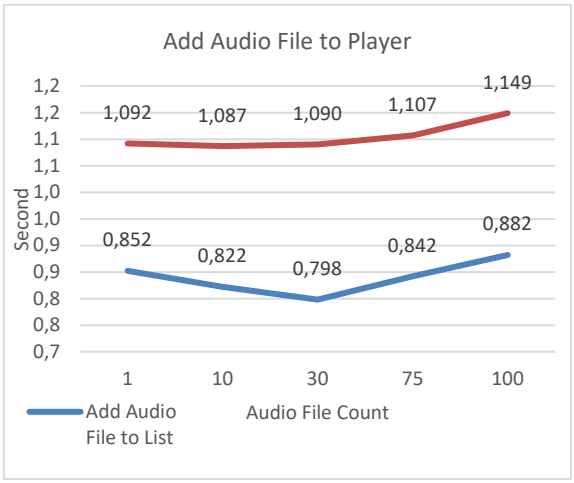

Fig. 5 Performance analysis graph of ordinary audio player with proposed model application about adding file.

The numeric values obtained in Table 2 are graphed in Figure 5 and Figure 6. As a general opinion, it is thought that performance will decrease as the number of audio files added to the wallet increases. But the measured results show that this is not the case. This is because when the user is asked to read a file from the music wallet, the password and iteration vector used to encrypt the file, which were previously created using the blockchain and the user Key, are recalculated. This value for each audio file is stored in a different column in the database, although the amount of data in the wallet increases, the calculation is done once, regardless of the number of audio files. In this way, it does not cause any noticeable loss of performance.

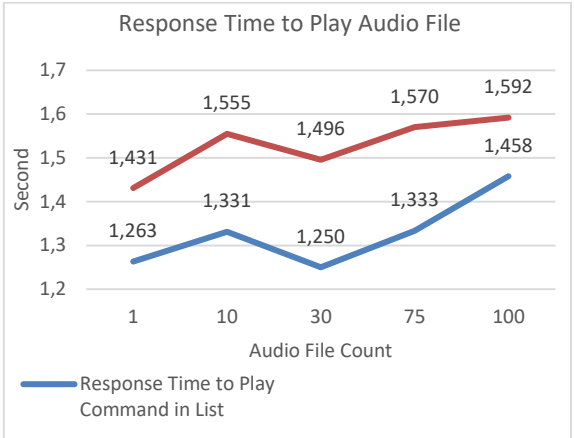

Fig. 6 Performance analysis graph of ordinary audio player with proposed model application about response time.

The file writing speed values of different sized audio files of the proposed model application are shown in Table 3.

Table 3 File write speed

Time (ms)	*File Size (MB)*	*Time (ms)*	*File Size (MB)*	*Time (ms)*	*File Size (MB)*
156	3,697842	225	6,101348	255	6,107774
182	4,847627	226	6,098997	257	7,204290
187	4,084016	228	6,261375	260	7,674181
190	5,067056	229	6,734713	270	7,875742
191	4,941668	230	5,497763	273	6,799915
194	4,735405	233	6,295856	274	7,089560
198	5,081476	236	6,866997	275	6,576097
204	5,476447	237	6,225639	277	7,040659
205	5,675813	238	6,615595	281	6,220623
207	4,608137	239	4,655784	294	7,328917
209	5,915931	242	6,559797	311	8,367888
210	5,753554	244	6,833142	324	5,910915
212	5,438204	245	4,952953	336	9,695118
215	5,939755	246	5,697756	348	8,564120
217	4,972388	248	6,375872	365	9,117081
218	5,575817	249	7,035017	368	9,657502
219	4,413786	250	6,581113	379	6,083301
222	5,476447	251	7,127872	387	9,196075
223	5,456385	252	5,910617	410	7,044421
224	5,921573	254	7,506475	415	7,255855

The reading speed values of different sized audio files of the proposed model application are shown in Table 4.

Table 4 File read speed

Time (ms)	*File Size (MB)*	*Time (ms)*	*File Size (MB)*	*Time (ms)*	*File Size (MB)*
9	4,28135	14	6,81348	20	6,92592
10	5,07959	15	6,81785	24	9,69511
11	5,22849	16	7,69016	41	6,09899
12	5,93720	17	8,03529	51	6,22555
13	6,22222	19	9,38729	61	7,87574

Effects of different sized audio files on writing and reading performance are measured by stopwatch class and graphics of gathered numeric results shown in Figure 7 and Figure 8. As a result of this analysis, the graph of the file size and the time spent for the process creates a positive meaningful linear line.

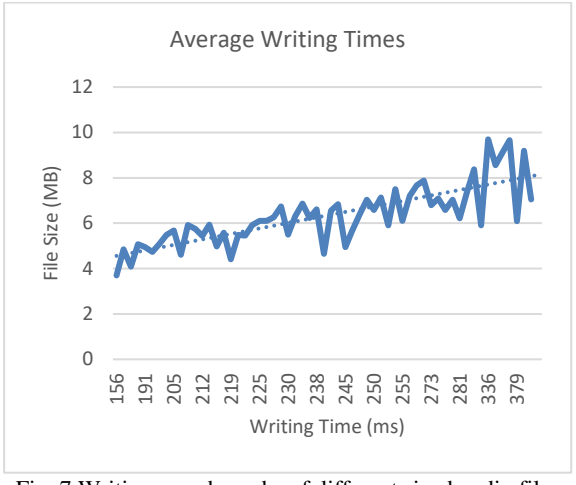

Fig. 7 Writing speed graphs of different sized audio files

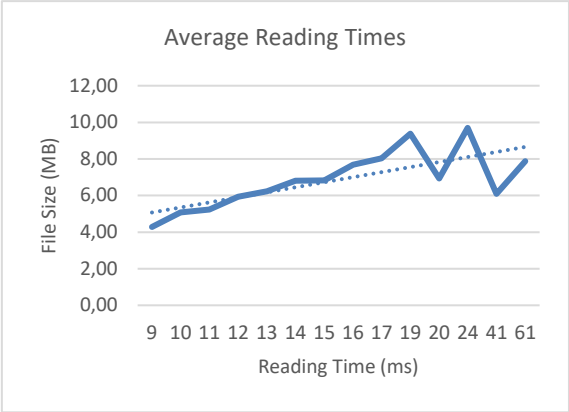

Fig. 8 Reading speed graphs of different sized audio files

5. Conclusions and Future Work

This article discusses the security measures and methods that can be provided on audio files in order to protect and secure the copyright of audio files. To ensure security, audio files are converted into different forms and stored in music wallet. The blockchain structure, which is recorded in a separate column in the database, contains all the data about the music content that will be added to it, and the key used in the encryption algorithm of the file is dynamically generated from the block chain. This method also increases the complexity and security of the stored file.

In this study, for the safe listening of music files, each decoded chain block was stored on RAM and the accuracy of the decoded file on RAM was compared with the RAW file and checked for data integrity. In addition, a music wallet model was developed using the blockchain structure, and each music file was stored in the wallet with interconnected Dynamic Encryption.

The performance benchmarking results of an ordinary audio file player with the proposed model application are acceptable considering the data security and data integrity it provides, although the results of the application in this study have lower values.

The subject matter of the work is not included in the subject matter of charging or paying royalties. We plan to parallelizing AES process and integrate the remuneration payment section into the current practice in our next work.

Competing interests

The authors have declared that no competing interests exist.

Authors' contribution

The idea design of this study belongs to ME. ME analyzed the results of the study and contributed to the revision of the article. RG wrote the code in the study, developed the

applications, conducted the experiments and wrote the article. All authors have read and approved the last article.

References

[1] P. K. Dhar and J. M. Kim., "Digital watermarking scheme based on fast Fourier transformation for audio copyright protection", *International Journal of Security and Its Applications*, vol. *5, no.* 2, pp. 33-48, 2011.

[2] J. Seok, J. Hong, and J. Kim, "A novel audio watermarking algorithm for copyright protection of digital audio", *etri Journal*, vol *24., no.*3, pp. 181-189, 2002.

[3] R. W. Ciptasari, K. H. Rhee, and K. Sakurai, "An enhanced audio ownership protection scheme based on visual cryptography", *EURASIP Journal on Information Security*, vol 2, no.1, pp. 2, 2014.

[4] M. Loytynoja, N. Cvejic, and T. Seppanen, "Audio protection with removable watermarking", In *2007 6th International Conference on Information, Communications & Signal Processing*, pp. 1-4, 2007.

[5] M. B. Andra, T. Ahmad, and T. Usagawa, "Medical Record Protection with Improved GRDE Data Hiding Method on Audio Files", *Engineering Letters*, vol.*25, no.*2, 2017.

[6] J. Wu, and N. K. Tran, "Application of blockchain technology in sustainable energy systems: An overview", *Sustainability*, vol.10, no.9, pp. 30-67, 2018.

[7] G. Zyskind, and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data", *In 2015 IEEE Security and Privacy Workshops*, pp. 180-184), 2015.

[8] W. E. I. She, Z. H. Gu, X. K. Lyu, Q. I. Liu, Z. Tian, and W. Liu, "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving", *IEEE Access*, vol.*7*, pp. 62058-62070, 2019.

[9] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities", *IEEE Internet of Things Journal*, vol.*6, no.*5, pp. 7702-7712, 2019.

[10] S. Kaushik, and A. Sinha, "Fog-Assisted Data Security and Privacy in Healthcare", In *Fog Computing for Healthcare 4.0 Environments,* Springer, Cham, pp. 315-336, 2021.

[11] S. Ravikumar, and D. Kavitha, "IoT based home monitoring system with secure data storage by Keccak–Chaotic sequence in cloud server", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, 2020.

[12] L. M. Kaufman, "Data security in the world of cloud computing", IEEE *Security & Privacy*, vol. *7, no.* 4, pp. 61-64, 2009.

[13] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks", *IEEE Wireless communications*, vol. *17, no.* 1, pp. 51-58, 2010.

[14] L. Bracciale, P. Loreti, E. Raso, M. Naldi, and G. Bianchi, "CoProtect: Collaborative Management of Cryptographic Keys for Data Security in Cloud Systems" In *ICISSP,* pp. 361-368, 2020.

[15] S. K. Saroj, S. K. Chauhan, A. K. Sharma, and S. Vats, "Threshold cryptography-based data security in cloud computing", In *2015 IEEE International Conference on Computational Intelligence & Communication Technology,* pp. 202-207, IEEE, 2015.

[16] H. Wang, S. Ma, H. N. Dai, M. Imran, and T. Wang, "Blockchain-based data privacy management with nudge theory in open banking", *Future Generation Computer Systems*, vol. *110*, pp. 812-823, 2020.

[17] A. Lazarovich, "Doctoral dissertation, Massachusetts Institute of Technology", *Invisible Ink: blockchain for data privacy*, 2015.

[18] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home", In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623), IEEE, 2017.

[19] 魏铭, 区块链" 技术在数字音乐版权中的应用初探, "A Preliminary Study on the Application of the Blockchain Technology in Digital Music Copyright", *Advances in Social Sciences*, vol. *9*, pp.172, 2020.

[20] P. W. Chen, B. S. Jiang, and C. H. Wang, "Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet", In *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* pp. 139-146, IEEE, 2017.

[21] A. Bessani, J. Sousa and M. Vukolić, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform", In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 1-2, 2017.

[22] R. D. Shelke and M. U. Nemade, "Audio watermarking techniques for copyright protection: A review", In *2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*, pp. 634-640, IEEE, 2016.

[23] T. Xu, X. Shao, and Z. Yang, "Multi-watermarking scheme for copyright protection and content authentication of digital audio", In *Pacific-Rim Conference on Multimedia*, pp. 1281-1286, Springer, Berlin, Heidelberg, 2009.

[24] R. Hrischev, "ERP systems and data security", In IOP Conference Series: Materials Science and Engineering, vol. 878, no. 1, pp. 012009), IOP Publishing, 2020.

[25] R. Kumar and R. Tripathi, "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model", Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, 2020.

[26] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain", *In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC),* vol. 2, pp. 359-364, IEEE, 2018.

[27] S. Zhao, and D. O'Mahony, "Bmcprotector: A blockchain and smart contract-based application for music copyright protection", *In Proceedings of the 2018 International Conference on Blockchain Technology and Application,* pp. 1-5, 2018.

[28] K. S. Lee and S. K. Kim, "Use of blockchain for music content copyright protection", In *Proceedings of the Korean Society of Broadcast Engineers Conference*, pp. 291-295, The Korean Institute of Broadcast and Media Engineers, 2019.

Citation: R. Gürfidan, M. Ersoy. *Blockchain-Based Music Wallet for Copyright Protection in Audio Files.* Journal of Computer Science & Technology, vol. 21, no. 1, pp. 11-19, 2021.
DOI: 10.24215/16666038.21.e02
Received: October 23, 2020 **Accepted:** February 5, 2021.