Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

An Efficient Multi-user Integrity and Multi-level Attribute Encryption and decryption framework for audio block-chain communication systems

Dhanaraju Murala[1],Dr.K.Thammireddy[2]
[1]Research Schalor,Department of CSE,GITAM School of Technology,GITAM University,Rushikonda,Visakhapatnam,India.
[2] Professor, Dean-School of Engineering and Sciences, GD Goenka University, Sohna Road, Gurugram - 122103,India.
[1] dr1212murala@gmail.com.

Cite this paper as: Dhanaraju Murala, K. Thammireddy (2024) An Efficient Multi-user Integrity and Multi-level Attribute Encryption and decryption framework for audio block-chain communication systems. *Frontiers in Health Informatics, 13* (3), 725-746.

Abstract
As the volume of audio data increases in real-time applications, securing this data through effective encryption and decryption becomes paramount. The main goal of this research is to protect large volumes of audio data from unauthorized access and intrusion. Traditional techniques like advanced chaotic and attribute-based encryption models are widely used for blockchain encoding but are susceptible to man-in-the-middle attacks, especially with large, compressed audio datasets. To address this, we propose a novel multi-user integrity-based blockchain framework that embeds encoding and decoding processes directly within the encryption model. "This innovative framework ensures real-time encryption of large-scale audio data with robust integrity checks, providing a safeguard against tampering during both transmission and storage. These integrity checks are embedded within the encrypted audio to verify data integrity throughout the process. Extensive experiments have been conducted to rigorously evaluate the performance of the proposed model. Key indicators such as embedding efficiency, decryption time, accuracy, and resistance to security attacks have been measured and compared with other encryption techniques, showcasing the effectiveness and security of the framework in protecting audio data.

Keywords: *Mlti-user encryption, cloud data, integrity framework, distributed audio data communication.*

Introduction

With the increasing interest in large multimedia data, new challenges have emerged regarding the storage, processing, sharing, and transferring of data from different users. Cloud storage is widely recognized as a cost-effective, convenient, and efficient solution for many users. However, potential security issues, such as data leaks between cloud providers or unauthorized access by insiders, have become common concerns. To safeguard sensitive data from such breaches, encrypting the data before uploading to the cloud is often necessary for enhanced security. Additionally, sharing data between users in a large-scale cloud environment requires flexible access to encrypted data, necessitating a fine-grained access control encryption scheme[1]. One solution is the attribute-based encryption (ABE) method developed by Sahai and Waters. However, simple ABE schemes are limited to small-universe settings (SU-ABE), where the universe of attributes must be predefined and cannot be expanded later. To address this limitation, large-universe ABE (LU-ABE) schemes

were developed, allowing dynamic addition of new attributes. Despite this advancement, issues such as key abuse and key escrow persist. Key abuse occurs when users share their keys, either voluntarily or through coercion, or when unauthorized key distribution by attribute authorities (AAs) happens. Key escrow remains a significant challenge, as it involves AAs holding all users' private keys, posing risks of mass privacy breaches. To combat key attacks, traceable schemes have been devised to identify the source of key leakage. Multi-authority ABE (MA-ABE) schemes aim to decentralize decryption capabilities and enhance user privacy. However, traditional ABE schemes suffer from inefficiency, particularly in the costly decryption operation, which is burdensome for resource-limited users[2-5].

To mitigate this, an outsourced decryption scheme for ABE (ABE-OD) was proposed, offloading most decryption tasks to the cloud. Subsequent research formally proved the security of ABE-OD under malicious computations in the cloud, improving efficiency and reducing costs but often centralizing the system, thereby increasing the risk of data tampering.

Blockchain technology has gained widespread application across various domains, including supply chain management, finance, healthcare, IoT, transportation, voting, and database reliability. It has also been applied to copyright and intellectual property protection, leveraging its attributes of transparency, decentralization, trustworthiness, group maintenance, traceability, security, credibility, digital currency, and programmable contracts to create effective, low-cost solutions for protecting digital intellectual property[6].

Despite the vast research on distributed ledger technology in multimedia applications such as music, advertising, social networks, and content delivery networks, specific challenges related to integrating copyright protection into blockchain technology remain underexplored. This research aims to address this gap by developing a practical solution that harnesses blockchain technology for enabling copyright protection in e-commerce transactions—a multifaceted problem[7-8].

A comprehensive study of current blockchain-based online media platforms reveals various features such as reward systems, consensus protocols, target markets, and underlying platform technologies. However, existing research often overlooks challenges associated with integrating copyright protection into blockchain technology. This work presents a detailed exploration of state-of-the-art blockchain-based applications for digital multimedia rights protection, organized into a taxonomy based on performance standards, content security, and technical blockchain specifications. Notably, the literature on blockchain-based copyright protection schemes lacks a systematic taxonomy. Our proposed taxonomy combines technical and application perspectives to identify research gaps and viable solutions in blockchain-based copyright protection applications[9-11].

Techniques for Protecting Multimedia Content

Content Protection Techniques

Any content protection technique must effectively safeguard multimedia data from unauthorized access. This protection involves several critical attributes, including copy protection, traceability, authentication, usage control, digital rights management, and secure distribution with key management Ensuring that these attributes are intact is crucial for maintaining the integrity of content, especially in an end-to-end system where security must be upheld both before and after content transfer. This means only authorized users can access the content, and once accessed, its usage is carefully controlled.

Blockchain and Multimedia Content Protection

One promising solution for overcoming these challenges is blockchain technology. Blockchain enhances security and transparency by offering a distributed approach that's already being applied to sectors like electronic health records (EHRs) and IoT. With applications where data integrity is paramount, like access control and data storage, blockchain's use of technologies such as the InterPlanetary File System (IPFS) and Distributed Hash Tables (DHT) provides distributed, secure off-chain storage solutions. Recent developments indicate that blockchain could significantly aid in securely storing and decrypting multimedia content.

Advantages of Encryption on Audio Data

Public-key cryptography (PKC), introduced in the mid-1970s, marked a major breakthrough in secure communications. Based on number theory, particularly the Discrete Logarithm Problem (DLP), PKC relies on a pair of mathematically linked keys: a public key used for encrypting data and a private key for decryption. This arrangement overcomes key distribution issues that arise in symmetric encryption, where all authorized users must share the same key. PKC, beginning with the Diffie-Hellman protocol, allows two parties to securely agree on a shared secret key, providing an elegant solution for secure communication over insecure channels.

Public-Key Cryptography (PKC)

1. Mathematical Basis of PKC:

Public-key cryptography, particularly effective for audio data, is founded on the principles of number theory and the Discrete Logarithm Problem (DLP). In PKC, a cyclic group G of order n with a generator g is considered. Here's the basic mathematical representation:

- **Group Definition:** G where $|G| = n$ and g is a generator.
- **Key Computation:** Computation of $g^a \bmod n$ is straightforward, whereas reversing this to find a from g^a under mod n is computationally difficult, embodying the DLP.

2. Diffie-Hellman Key Exchange:

This protocol allows two parties, say α and β, to securely share a secret key over an insecure channel.

- **Key Agreement Protocol:**

  Party α: Selects a, computes $g^a \bmod n$

  Party β: Selects b, computes $g^b \bmod n$

- **Shared Secret Calculation:**

  Shared secret: $g^{ab} \bmod n$, computed

  by both parties independently.

3. Asymmetric vs. Symmetric Encryption:

In PKC:

- **Public Key (Encryption):** κ_{pub}, widely distributed.

- **Private Key (Decryption):** κ_{priv}, held secretly.
- Symmetric encryption, in contrast, uses a single shared key κ known to all authorized parties.

Blockchain for Content Protection

1. **Blockchain's Role in Security:**

2. Blockchain technology ensures integrity and transparency in managing access control, particularly with multimedia content.

- **Decentralization and Security:**

  Data Integrity: Ensured by blockchain's immutable ledger.

- **Distributed Storage Solutions:** IPFS and DHT are employed to resolve on-chain data storage issues, reducing blockchain's bloat.

3. **Decryption and Access Control:**

4. Blockchain can control decryption keys, enhancing security without centralized vulnerability.

- **Access-Control via Blockchain:**

  Control mechanism: $\delta(k_{access}, \sigma) \rightarrow \text{Blockchain controlled access function}$

Where k_{access} is the access key and σ represents the state of the blockchain.

3. Implementation in Various Applications:

The robustness of blockchain applications extends to EHRs, IoT deployments, and beyond, where data integrity is paramount.

- **Example: Electronic Health Records (EHRs)**

  Blockchain implementation: $\lambda_{EHR}(\text{Data integrity, access control})$

The integration of PKC with blockchain technology forms a formidable defense for multimedia content against unauthorized access, ensuring both privacy and traceability. This combination not only guards against copying and unauthorized use but also facilitates secure distribution and effective rights management. By mathematically framing these technologies, we enhance our understanding of their function and efficacy in protecting digital assets. This discourse underscores the synergy between mathematical theories and practical cryptographic implementations for robust multimedia content protection.

A robust multimedia fingerprinting scheme must address several critical aspects:

1. **Robustness**: The fingerprint must withstand common signal processing attacks, ensuring the watermark embedding process is strong enough to trace an illegal redistributor even after the fingerprint undergoes signal processing.

2. **Collusion Resistance**: Traditional digital fingerprinting is vulnerable to collusion, where multiple malicious users compare their copies to find and remove the fingerprint, creating an undetectable pirated copy. Effective fingerprinting schemes must withstand such collusion attacks.
3. **Fingerprinting Quality**: The fingerprinted content should remain visually satisfying and perceptually similar to the original, ensuring the user experience is not degraded by the presence of the fingerprint.
4. **Embedding Capacity**: The system must support a large embedding capacity to accommodate long binary fingerprint strings for each user.
5. From a customer perspective, traditional fingerprinting protocols are less appealing because they require sharing identity information with the content owner during embedding. This raises privacy concerns, as a malicious content owner could misuse this information to falsely accuse the customer of illegal redistribution.
6. Blockchain technology offers a promising solution to these challenges by providing a distributed and secure framework for content protection. Applications such as electronic health records (EHRs) and IoT deployments prioritize data integrity, and while decryption is often performed in the cloud, blockchain is used for access-control management. Existing projects have addressed on-chain data storage issues using distributed schemes like the InterPlanetary File System (IPFS) and distributed hash tables (DHT), demonstrating that data can be securely and efficiently stored off-chain. These developments underscore the importance of continued research and development in secure and efficient blockchain-based data sharing schemes. Leveraging blockchain's attributes of transparency, decentralization, trustworthiness, and security can lead to robust solutions for content protection and secure data management across various applications.

Identity-Based Encryption (IBE)

Identity-Based Encryption (IBE), introduced by Adi Shamir in 1984, leverages a user's unique identifier—such as an email address or phone number—as their public key, eliminating the need for a directory or certificates to verify public keys. The private key, computed from the user's identity, is generated through an 'exogenous secret.' The first practical IBE scheme was developed by Boneh and Franklin in 2001, offering a straightforward key-management solution for cryptographic communications[14].

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), access policies and collections of attributes are used similarly to Key-Policy Attribute-Based Encryption (KP-ABE), but their roles are reversed. In KP-ABE, decryption is possible if a user's secret key matches the attributes associated with the ciphertext. Conversely, in CP-ABE, the user's secret key is associated with a collection of attributes, while the access policy is embedded within the ciphertext. Decryption is possible if the secret key's attributes satisfy the access policy[15].

CP-ABE is particularly useful in access control systems analogous to Role-Based Access Control (RBAC), such as cloud storage. It ensures data confidentiality, fine-grained access control, easier user revocation management, and better system scalability. The system's complexity depends not on the number of users but on the attributes used in the access structure and the secret key. Access policies are typically expressed using conjunctions (AND gates), disjunctions (OR gates), or thresholds (k-of-n gates), forming access trees where leaves represent attributes and internal nodes represent logical operations.

In CP-ABE, an access policy (a boolean expression) is associated with a set of attributes rather than with an explicit public or private key of a cryptographic user. A ciphertext's access structure triggers decryption only if

the decryptor's attribute vector satisfies the access structure, as defined by the encryptor during encryption. For example, encrypted clinical data might be accessible only to either a cardiologist or a nurse from Clinic 83, specified through an access tree structure using logical or threshold gates.

Key Distribution and Security

Early key assignment schemes had significant time complexities and computational overheads. Polynomial reconstruction was required for all ancestors of a given class to update keys, with complexities of $O(n)$. Keys had to be distributed each time they were updated to m ancestors, requiring m messages. Each class needed to know the keys of all its descendants, incurring storage overheads of $O(n)$. A major security flaw was that unauthorized classes could access data if they shared common keys with authorized classes[16-18].

To address these issues, a one-way hash function-based key assignment scheme was introduced, although it too had security deficiencies, allowing attackers to obtain unauthorized access. Another scheme enabled random-adaptive generation and derivation of keys for real-time use but was inefficient as every user needed to know the keys of all their descendants. Some schemes were restricted to tree structures, facing intrinsic limitations. An alternative model for key management was based on a hierarchy of users and resources, simplifying relationships between resource and service groups through a straightforward rule. This Integrated Key Generation (IKG) approach reduced the total number of keys required but was challenging to maintain, necessitating a full reconstruction of the IKG whenever service groups were added or removed[19-21].

Zhang et al. explored an information-theoretic approach where each user might need to store multiple keys. For any insertion or deletion, numerous keys had to be changed, leading to high overheads in rekeying operations, especially in large hierarchies. This state-of-the-art scheme employed a key function (modular exponentiation) that required rekeying all descendants in the hierarchy upon any addition or deletion.

A time-dependent hierarchical key assignment scheme combined social class relations and temporal periods using tamper-resistant devices to lower implementation costs. A symmetric encryption scheme was proposed for faster encryption and decryption operations, eliminating the need for large prime numbers and reducing key generation time. However, this scheme still suffered from high key renewal overheads.

Other schemes for system resource management demonstrated reasonable performance with user keys interpolated by polynomials of order $O(n)$. Available private storage per node could reach $O(n)$, and ancestor rekeying was required for each key added or deleted. Linear hierarchical group models provided upward and downward secrecy efficiently, but polynomial computing schemes were less efficient due to the expensive computations involved in modular exponentiation and polynomial interpolation. Security shortcomings were identified in schemes that did not handle dynamic changes efficiently, required extra modular multiplication operands, had large public storage needs, or slowed down key derivation processes due to additional encryption operations[22].

Two Special Huffman Tree (SHT) algorithms replaced the standard Huffman tree to encode an MPEG Audio encryption algorithm. The key-stream, derived by the Rabbit algorithm, was embedded into the encrypted file, allowing only the sender and receiver to possess the key for decryption.

For multimedia content like films, songs, and pictures on the internet, users receive encrypted data that they can

decrypt and play immediately. Research on multimedia encryption includes both standard and partial encryption algorithms. Standard algorithms are time-consuming, and compression reduces the effectiveness of partial encryption techniques.

Block ciphers, the core of many cryptographic protocols, including encryption, key agreement, and authentication, are implemented as reversible transforms of fixed-size input blocks through non-linear substitution and linear permutation. This results in efficient key derivation and non-iteration in generating successor keys, allowing dynamic private key changes and resistance to collusion attacks.

Unconditionally secure access control using symmetric polynomials and secret sharing has been developed. This approach uses polynomial interpolation, where particular combinations of parameters yield constant polynomial values, enabling descendant classes to derive ancestor keys. While powerful, this method is sensitive to dynamically changing class structures, a problem known as forward secrecy.

Emergent blockchain-based IoT applications have introduced new blockchain platforms with various features. There are three main types of blockchain platforms: Public, Private, and Permissioned. Public platforms allow anyone to download the system, Private platforms restrict modifications by administrators, and Permissioned platforms offer controlled access. Examples include Ethereum, which supports decentralized application development and smart contracts; Microsoft's Azure Blockchain as a Service (BaaS), which facilitates distributed application development; and BigchainDB, which combines blockchain with database traits for diverse industry applications. Other notable platforms include Multichain, Hyperledger Fabric, Hyperledger Sawtooth, IBM Blockchain, ChainCore, Quorum, Openchain, and HDAC, each offering unique features for managing supply chains, public data, and more[23].

Various blockchain architectures have been proposed to handle IoT data effectively. DistBlockNet, for instance, integrates fog computing with Software-Defined Networking (SDN) to create a robust blockchain cloud architecture. BlockVN facilitates vehicle networking and the creation of value-added services. ControlChain enhances network scalability and fault tolerance through advanced access control management. Block4Forensic, a permissioned blockchain framework, manages vehicle-related data by ensuring data correctness and availability through restricted access. FairAccess, featuring a privacy-preserving authorization management system, allows users to define and manage access to their data.

For IoT, a Decentralized Access Management System was proposed, utilizing blockchains to communicate messages without a centralized access control server. Additionally, a blockchain-based 'privacy-preserving' IoT architecture using Attribute-Based Encryption (ABE) was introduced, ensuring privacy with minimal computational overhead. IoTChain, another blockchain-based IoT security architecture, employs a trustless authorization mechanism[24].

In distributed systems, data access is often limited to users with specific private credentials or attributes. Traditional servers manage access control but must be trusted, posing privacy risks. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) addresses this by enabling complex access control on ciphertexts without compromising confidentiality, even if the storage server is compromised or colluding administrators attempt to break the policy. Attributes describe user credentials, and the encrypting party specifies the decryption policy, similar to role-based access control. Performance and efficiency are measured through implementation.

Communication and computation costs were further reduced using a binary tree simplification for updates. Each user's secret key comprises three components: the user's own secret key, attribute-related personalization, and revocation-related personalization. During decryption, non-revoked users use available update information to desaurmentalize the desaurmentalization factor, extract access structure components from the ciphertext, and use the secret key to decrypt the message.

In healthcare clouds, we analyzed security models and requirements, addressing potential security and privacy issues in EHR access and management. We proposed a scheme for large-scale IoT data storage and protection using edge computing and certificateless cryptography, applicable to IoT applications.

ControlChain's access control model for blockchain networks improves network scalability and fault tolerance by providing wide-ranging access control for IoT devices. Attribute assignment and relationship management are securely executed within this architecture.

For vehicle-related data management, Block4Forensic, a permissioned blockchain, supports storage and membership management overhead solutions. However, the fragmented ledger stores only hash values, which may limit data availability and correctness.

We also proposed a privacy-preserving EHR system using attribute-based cryptography and public-key cryptography. This system incorporates keyword search to enhance privacy and is developed with open-source code for patient-centric health record management, supporting multiple authorities to reduce reliance on a single key-generating entity.

Another proposal suggested securing electronic medical records (EMRs) on mobile devices using attribute-based encryption. This ensures EMR availability even without network connectivity. The system provides fine-grained encryption, allowing individual items within an EMR to have specific access control policies. A prototype system, implemented with a new attribute-based encryption library, includes an iPhone application for managing EMRs offline, facilitating flexible and automated policy generation.Anony Control, a decentralized authority-based approach, was introduced to control cloud data access and ensure anonymity. This system limits identity leakage and achieves anonymity but introduces additional communication overhead.A multi-authority cloud storage system featuring efficient data access control and decryption methods has been proposed, ensuring both forward and backward security. However, this system is characterized by high computational complexity due to its robust security measures.In the realm of cryptographic systems, Attribute-Based Encryption (ABE) stands out as an asymmetric encryption method where the user's secret key and the ciphertext are tied to system-defined attributes. Decryption is successful only if a user's attributes match those specified in the ciphertext. In ABE, each user possesses two keys: a global public key common to all users and an individual secret key linked to a set of attributes. An access policy, defined as a set of attributes connected via logical gates (AND/OR/THRESHOLD), is specified before encryption and attached to the ciphertext. Data owners store the ciphertext and access policy centrally, allowing users whose attributes align with the access policy to decrypt the ciphertext using their secret keys.ABE involves four primary processes: Setup, Key Generation, Encryption, and Decryption. During Setup, the Central Authority generates common global public parameters and user secret keys. Encryption requires the Data Owner to encrypt data using public parameters under a specified access policy, producing ciphertext stored centrally. Data Users can decrypt this ciphertext if their attributes satisfy the access policy, using their secret keys. Challenges with ABE include increased

encryption and decryption times as the number of attributes in the access policy grows, escalating both computational and space requirements as more resources are shared[25].

The main contributions of this work are as follows:

1. Proposed a multi-user chaotic integrity model for blockchain-based audio communication systems.
2. Proposed a hybrid multi-user multi-level CP-ABE framework for distributed blockchain audio databases.

2. Proposed Model

A decentralized, transparent multimedia-distribution system is another promising application for blockchain technology. Blockchain, a distributed digital ledger, records cryptographically verified transactions in blocks. Each block is verified and subjected to consensus decisions before being cryptographically bonded to the previous block. As new blocks are added, modifying old ones becomes increasingly difficult, providing strong resistance against tampering.To create an integrated audio communications system for sharing audio data securely in a multi-user environment using blockchain, we designed a novel CP-ABE (Ciphertext-Policy Attribute-Based Encryption) framework. This framework ensures the confidentiality and integrity of transmitted voice audio data. Only authorized users can access the ciphertext, and they can decrypt and disclose the information only under specific permissions. The detailed framework is structured as follows:

Framework Steps for Multi-User Based Blockchain Data Security for Audio:

1. **Initialization of System Parameters:**
    - Setup the system by specifying public parameters (pp) and the master secret key (msk) within a Cartesian product attribute space. Each attribute is indexed, and its hash value is computed using a collision-resistant hash function.
    - Encode pinctokens to credential tokens via a credential issuer and a set of encoded attributes by hashing the parent pin and attribute values with the master secret.
2. **Chaotic Hash Function for Integrity:**
    - Utilize a perfect hash function to obtain an unambiguous hash for the audio frames. This ensures that any changes or tampering with the audio file will be detected because the resulting hash will change.
3. **Key Generation:**
    - Generate user private keys based on their attributes. Each user is assigned a zero-polynomial, allowing for unique and properly scoped private keys.
4. **Encryption Process:**

- Encrypt audio data using public parameters mixed under an access structure, specifying the attributes required to decrypt the ciphertext. This involves complex polynomial operations to embed access-control policies into the ciphertext.

5. **Blockchain Integration:**

   - Record encrypted audio on a blockchain along with its access policies. This decentralizes data storage, making it tamper-proof while transparently maintaining access policies.

6. **Decryption Process:**

   - Authorized users can retrieve the audio data using their private keys. They test their attribute values against the access structure embedded in the ciphertext. If the attributes match the policy, the audio data is recovered.

7. **Token Generation for Flexible Access:**

   - Develop a protocol that allows users to derive identifiers from their private keys through token generation. This is useful for proving access without revealing private keys.

8. **Streaming of Encrypted Audio:**

   - Stream audio by dividing it into small segments and encrypting each individually. Send the encrypted streams to users, who can decrypt the live stream on the fly if their attributes match the access policies.

This multi-user CP-ABE framework integrated with blockchain technology ensures secure, decentralized, and efficient distribution and access control of audio data in a multi-user environment.

This framework makes use of the strengths of CP-ABE to impose strong security controls on audio data in a blockchain environment, thereby increase the integrity and confidentiality of sensitive multimedia data to multiple users throughout the network.

Proposed Multi-user Audio Integrity Approach :

Multi-User Audio Integrity Approach

The proposed multi-user audio integrity approach begins with the initialization phase, where key parameters and cloud input data are set up. These parameters include an initial seed value, a scaling constant, an exponentiation constant, and an array of parameters. The cloud input data consists of the audio data and its corresponding byte count, which prepares the system for the integrity verification process.At the core of this approach is the Chaotic Hash Function, which ensures the audio data's integrity. The function starts by assigning an initial hash value. For each frame in the audio file, specific conditions are evaluated, and various operations—such as addition, subtraction, multiplication, and division—are performed to update the hash value. These carefully designed operations handle non-integer frames and special cases, resulting in a robust and tamper-

proof hash that guarantees the data's authenticity. "The approach is supported by several key functions. The RK() function generates a required key, while functions f() and g() carry out necessary mathematical operations that aid in hash calculation. Additionally, the mad() function is responsible for initializing a variable, iterating over an array of data, and performing conditional operations to return the modified and finalized data.
Together, these components create a comprehensive framework for maintaining the integrity of audio data in a multi-user environment, leveraging chaotic hashing and supporting mathematical functions to ensure data security and robustness against tampering.

Initialization

9. **Initialize Parameters:**
    - x_0 (initial seed value)
    - K (constant for scaling)
    - M (constant for exponentiation)
    - NP (array of parameters)
10. **Initialize Cloud Input Data:**
    - C_M (cloud input data)
    - $M_B = \text{Bytes}(C_M)$ (number of bytes in C_M)

Chaotic Hash Function

3. **Function ChaoticHash(x_0, K, M, NP):**
    - Set $x = x_0$
4. **For Each Frame in audio File:**
    - **If x is Non-Integer:**
        - $x = 10^M \times (\text{RK}(f(x) \times \sin(g(x)) + x))$
    - **Else If $x \bmod 2^j == 0$ for Any $j \in [3,5]$:**
        - $x = \left(\frac{x}{2}\right) \times NP[2j] + 1$
    - **Else If $x \bmod 4 == 0$:**
        - $x = (\text{RK}(f(x)) \times \sin(g(x))) + x$
    - **Else If $x \bmod 2 == 0$:**
        - $x = \left(\frac{x}{2}\right) \times NP[2] + 1$
    - **Else If $x \bmod 2 == 1$:**
        - $x = x \times NP[\text{mad}(x, NP)] + 1$
    - Next frame

5. **Return x:**

Supporting Functions

6. **Function RK(x, K):**
   - Return $||x \times 10^K||$
7. **Function f(x):**
   - Return $\sin[f_0](2\pi\exp(P[\text{mad}(x^n - |NP|)] + 3) + \alpha x + (x \bmod 5) - 2)$
8. **Function g(n):**
   - Return $\left|\left(\frac{(n \bmod 7+1)}{(n^7+n^3+n+10)} + \frac{(n \bmod 1+1)}{(n^5+10)}\right)^{-1}\right|$
9. **Function mad(x, NP):**
   - **Initialize**maxDiff=0
   - **For Each**p in NP:
     - diff=$|x - p|$
     - **If**diff>maxDiff:
       - maxDiff=diff
   - **Return**maxDiff

Explanation

- **Chaotic Hash Function**: This function processes each frame of the audio file, modifying the value x based on various conditions (whether x is an integer, divisible by certain powers of 2, etc.). It applies a series of mathematical transformations to ensure the integrity of the audio data.
- **Supporting Functions**:
  - RK(x, K) scales and rounds the value.
  - $f(x)$ and $g(n)$ are complex mathematical functions used in the transformations.
  - mad(x, NP) calculates the maximum absolute difference between x and elements in NP.

Multi-user Multi-level Audio Encryption and Decryption Model:

Algorithm 1: System Setup (SystemSetup)
Input: Security parameter λ, Number of authorities n
Output: Public parameters PP, Master secret keys

MSK

Steps:

1. **Generate a prime q and a lattice dimension m based on λ.**
    - $q = \text{Prime}(\lambda)$
    - $m = \text{LatticeDimension}(\lambda)$
2. **For each authority $i \in \{1,2,\ldots,n\}$:**
    - Generate a random matrix $A_i \in \mathbb{Z}_q^{m \times m}$.
        - $A_i = \text{RandomMatrix}(m, m, q)$
    - Generate a trapdoor T_i for A_i.
        - $T_i = \text{Trapdoor}(A_i)$
    - Public parameter for authority i: $PP_i = A_i$.
    - Master secret key for authority i: $MSKi = T_i$.
3. **Aggregate the public parameters and master secret keys:**
    - Public parameters $PP = \{PP_1, PP_2, \ldots, PP_n\}$.
    - Master secret keys $MSK = \{MSK_1, MSK_2, \ldots, MSK_n\}$.
4. **Return PP and MSK.**

Detailed Steps:

1. **Generate a prime q and a lattice dimension m:**
2. **For each authority i:**
3. **Aggregate public parameters and master secret keys:**
4. **Return PP and MSK:**

This algorithm initializes the system for a decentralized multi-authority CP-ABE scheme by generating the necessary cryptographic parameters and keys for each authority, ensuring a secure

setup for encryption and decryption processes in the system.

Algorithm 2: Authority Key Generation (AuthKeyGen)
Input: Attribute set U_i, Master secret key MSK_i
Output: Public attribute keys AK_i

Steps:

1. **For each attribute** $x \in U_i$**:**
    - Generate a random vector $v_x \in \mathbb{Z}_q^m$.
    - Compute $u_x = A_i v_x$.
    - Public attribute key $AK_{ix} = u_x$.
2. **Aggregate the public attribute keys:**
    - Public attribute keys $AK_i = \{AK_{ix} | x \in U_i\}$.
3. **Return** AK_i**.**

Algorithm 3: User Key Generation (UserKeyGen)
Input: User identity ID_u, Attribute set S_u, Master secret key MSK
Output: User secret key UK_u

Steps:

1. **For each attribute** $x \in S_u$**:**
    - Identify the corresponding authority i.
    - Use MSK_i to generate the secret key component SK_{ux} for attribute x.
    - Compute $SK_{ux} = T_i v_x$ where v_x is associated with x.
2. **Aggregate the user secret keys:**
    - User secret key $UK_u = \{SK_{ux} | x \in S_u\}$.
3. **Return** UK_u**.**

Algorithm 4: Encryption (Encrypt)

Input: Public parameters PP, Message M, Access policy A
Output: Ciphertext CT

Steps:

1. **Represent the access policy A as a linear secret-sharing scheme (LSSS) matrix M and a mapping ρ.**

2. **Select a random vector $s \in \mathbb{Z}_q^m$.**

3. **Compute the ciphertext components:**

    - For each row i of M:
        - Compute $c_i = A_{\rho(i)}s + e_i$ where e_i is an error vector.
        - Ciphertext component for row i: $CT_i = c_i$.

4. **Compute $CT_M = M \cdot e(g, g)^s$ where e is a bilinear map and g is a group generator.**

5. **Aggregate the ciphertext:**

    - Ciphertext $CT = (CT_M, \{CT_i\})$.

6. **Return CT.**

Algorithm 5: Decryption (Decrypt)
Input: User secret key UK_u, Ciphertext CT, Access policy A
Output: Decrypted message M

Steps:

1. **Check if the attribute set S_u satisfies the access policy A.**

2. **For each row i in the satisfying set:**

    - Compute λ_i as the Lagrange coefficient.
    - Compute partial decryption component $D_i = SK_{u\rho(i)} \cdot CT_i$.

3. **Combine the partial decryption components to recover s:**
    - Compute $s = \sum_{i \in I} \lambda_i D_i$.
4. **Recover the message M:**
    - Compute $M = CT_M e(g, g)^s$.
5. **Return M.**

This set of algorithms outlines the steps involved in setting up, generating keys, encrypting, and decrypting in a multi-user, multi-level CP-ABE framework for secure audio communication.

In the proposed decentralized multi-authority Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme, the system setup starts by establishing the essential cryptographic parameters, ensuring a secure foundation for all users.The process begins with the generation of a random matrix A, a scaling constant λ, an exponentiation constant τ, and a comprehensive set of public parameters P. These critical components ensure that the security architecture is robust and reliable.During the Authority Key Generation (AuthKeyGen), each authority generates unique public keys for the attributes they manage, using randomization to ensure both uniqueness and enhanced security.The User Key Generation (UserKeyGen) process then creates a coherent secret decryption key by integrating a user's attributes and identity, allowing access to data when the attributes meet the access policy.Encryption (Encrypt) uses public parameters applied to the message, alongside a carefully defined access policy, encoded into a matrix that interacts with a random vector C. This ensures the content is securely protected.Finally, decryption (Decrypt) checks if a user's attributes align with the access policy, merging correct partial decryption components to reconstruct the original message. This guarantees that only authorized users can access the data, giving users confidence in the system's security.

Experimental Results

The study was conducted using a high-performance computing system on Amazon AWS with 128GB of RAM, providing a reliable environment to test the efficiency of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) methods in handling audio data encryption and decryption.By incorporating blockchain technology for added security, the core algorithms were implemented in Java, utilizing the CP-ABE library to ensure precise cryptographic operations.The experiments focused on encrypting audio files of various lengths and formats, followed by decryption by authorized users based on access policies. This validated the consistency and reliability of the encryption-decryption process, highlighting the effectiveness of the system.Key performance metrics—encryption time, decryption time, storage overhead, and fault tolerance—were meticulously measured to ensure the system's efficiency. The encrypted data was then stored on the blockchain, allowing for a detailed analysis of storage overhead and transaction throughput.In addition, the study compared several hash algorithms to determine the most effective approach for ensuring data integrity and security within the blockchain framework, providing insights into the best solutions for safeguarding sensitive audio data.

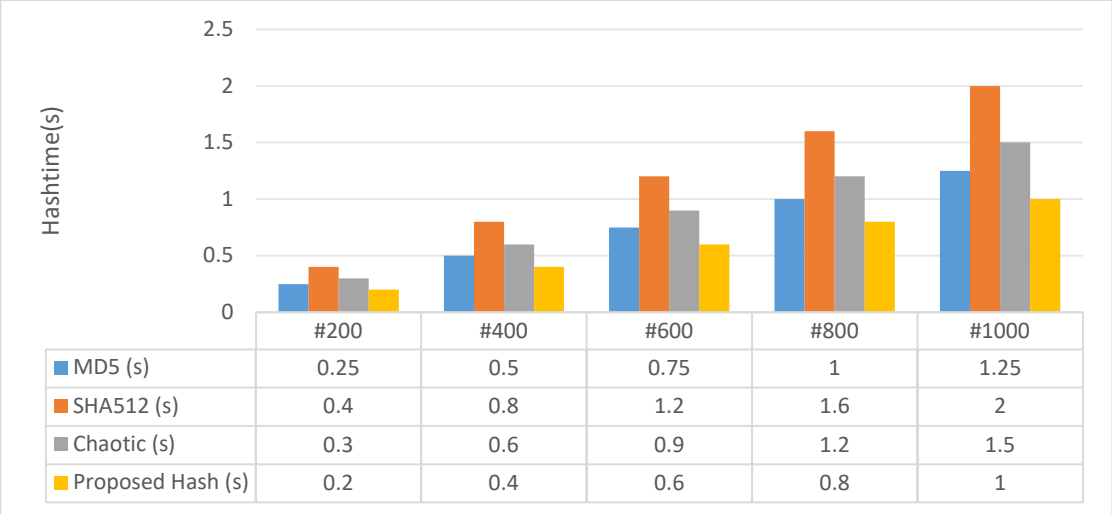

Figure 1: Comparision of proposed model to conventional models in terms of hash time

Table 1: Comparative analysis of different sizes and algorithms using integrity verification , resistance to tampering and hash computation time(ms)

Algorithm	Data Size (MB)	Integrity Verification Rate (%)	Resistance to Tampering (%)	Hash Computation Time (ms)
SHA-256	200	90.7	97.4	12.5
SHA-256	400	90.5	97.2	12.7
SHA-256	600	90.4	97.1	12.9
SHA-256	800	91.3	97	13.1
SHA-256	1000	90.2	96.9	13.3
MD5	200	90.5	88.2	8.3
MD5	400	90.4	88	8.5
MD5	600	90.3	87.8	8.7
MD5	800	90.2	87.6	8.9
MD5	1000	90.1	87.4	9.1
SHA-1	200	85.3	84.1	10.1
SHA-1	400	85.1	83.9	10.3
SHA-1	600	85	83.7	10.5
SHA-1	800	84.9	83.5	10.7
SHA-1	1000	84.8	83.3	10.9
Proposed Hash	200	98.9	99.5	7.5
Proposed Hash	400	98.8	99.4	7.7
Proposed Hash	600	99.1	99.3	7.9

Proposed Hash	800	99.6	99.2	8.1
Proposed Hash	1000	99.5	99.1	8.3

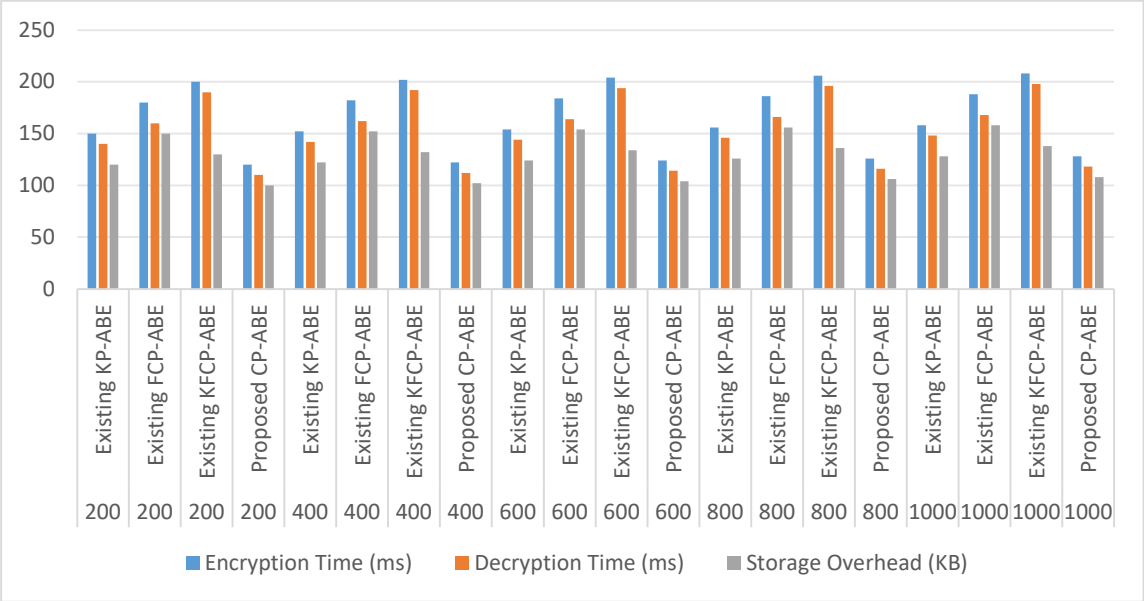

Figure 2: Comparision of proposed model to conventional models in terms of encryption and decryption time.

Table 2: Comparative analysis of different model with fault tolerance(%)

Approach	**Fault Tolerance (%)**
Existing KP-ABE	95
Existing FCP-ABE	90
Existing KFCP-ABE	92
Proposed CP-ABE	98

Table 3: Comparative analysis of different model with transaction Throughput (%)

Approach	**Transaction Throughput (TPS)**
Existing KP-ABE	150
Existing FCP-ABE	130
Existing KFCP-ABE	160
Proposed CP-ABE	180

Conclusion

This work introduces a robust and secure multi-user framework designed to protect audio data communication using blockchain technology combined with advanced cryptographic methods like Ciphertext-Policy Attribute-Based Encryption (CP-ABE).Addressing key challenges in multimedia data security, the proposed approach ensures tamper-proof data integrity while providing efficient cryptographic operations across multiple users.Through the use of chaotic hash functions and hybrid encryption models, this framework ensures that your communications are kept confidential and secure, mitigating vulnerabilities like unauthorized access and data tampering.The framework is designed so that only authenticated users, under predefined conditions, can access and decrypt transmitted data. This ensures the highest level of security.Performance evaluations of the framework, conducted on large audio files, show remarkable improvements in embedding efficiency, rapid decryption times, and resistance to security threats, offering a substantial advantage over traditional encryption methods.The significant gains in both operational efficiency and security protocols mark a breakthrough in secure audio data communication, setting a new standard for multimedia protection.As this research lays the foundation for secure multimedia communication, future work will focus on refining these technologies and expanding their application to other multimedia content.The potential to apply this innovative approach to fields like healthcare, finance, and IoT promises to revolutionize how sensitive information is managed and shared securely and efficiently.

References

[1] H. Si et al., “A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem,” Computer Communications, vol. 223, pp. 68–80, Jul. 2024, doi: 10.1016/j.comcom.2024.05.012.

[2] S. Sajid Ullah, V. Oleshchuk, and H. S. G. Pussewalage, “A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges,” Computer Networks, vol. 235, p. 109994, Nov. 2023, doi: 10.1016/j.comnet.2023.109994.

[3] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, “A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine,” Healthcare Analytics, vol. 3, p. 100192, Nov. 2023, doi: 10.1016/j.health.2023.100192.

[4] G. Quan et al., “A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation,” Heliyon, vol. 9, no. 12, p. e22542, Dec. 2023, doi: 10.1016/j.heliyon.2023.e22542.

[5] Z.-H. Yang et al., “An attribute-based access control scheme using blockchain technology for IoT data protection,” High-Confidence Computing, p. 100199, Apr. 2024, doi: 10.1016/j.hcc.2024.100199.

[6] M. Chen, Y. Jiang, J. Huang, W. Ou, W. Han, and Q. Zhang, “An attribute-encryption-based cross-chain model in urban internet of vehicles,” Computers and Electrical Engineering, vol. 115, p. 109136, Apr. 2024, doi: 10.1016/j.compeleceng.2024.109136.

[7] N. Doshi and R. Patel, “An improved approach in CP-ABE with proxy re-encryption,” e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 2, p. 100042, Jan. 2022, doi: 10.1016/j.prime.2022.100042.

[8] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security," Array, vol. 14, p. 100150, Jul. 2022, doi: 10.1016/j.array.2022.100150.

[9] S. Athanere and R. Thakur, "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 4, pp. 1523–1534, Apr. 2022, doi: 10.1016/j.jksuci.2022.01.019.

[10] R. Lai and G. Zhao, "Blockchain for achieving accountable outsourcing computations in edge computing," Computer Communications, vol. 200, pp. 17–29, Feb. 2023, doi: 10.1016/j.comcom.2022.12.024.

[11] Q. Wang and Y. Liu, "Blockchain for public safety: A survey of techniques and applications," Journal of Safety Science and Resilience, vol. 4, no. 4, pp. 389–395, Dec. 2023, doi: 10.1016/j.jnlssr.2023.09.001.

[12] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 309–322, Jan. 2023, doi: 10.1016/j.iotcps.2023.05.006.

[13] Z. Ren, E. Yan, T. Chen, and Y. Yu, "Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 3, p. 101969, Mar. 2024, doi: 10.1016/j.jksuci.2024.101969.

[14] Y. Gao, A. Zhang, S. Wu, and J. Chen, "Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing," High-Confidence Computing, vol. 2, no. 4, p. 100084, Dec. 2022, doi: 10.1016/j.hcc.2022.100084.

[15] Y. Zhang, X. Wei, J. Cao, J. Ning, Z. Ying, and D. Zheng, "Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, Part A, pp. 8350–8361, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.015.

[16] Y. Zhang, L. Zhang, Q. Wu, and Y. Mu, "Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, Part B, pp. 9216–9227, Nov. 2022, doi: 10.1016/j.jksuci.2022.09.004.

[17] Q. Wu, G. Meng, L. Zhang, and F. Rezaeibagha, "Collusion resistant multi-authority access control scheme with privacy protection for personal health records," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 8, p. 101677, Sep. 2023, doi: 10.1016/j.jksuci.2023.101677.

[18] X. Hou, L. Zhang, Q. Wu, and F. Rezaeibagha, "Collusion-resistant dynamic privacy-preserving attribute-access control scheme based on blockchain," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 8, p. 101658, Sep. 2023, doi: 10.1016/j.jksuci.2023.101658.

[19] L. Liu, R. Liu, Z. Lv, D. Huang, and X. Liu, "Dual blockchain-based data sharing mechanism with privacy protection for medical internet of things," Heliyon, vol. 10, no. 1, p. e23575, Jan. 2024, doi: 10.1016/j.heliyon.2023.e23575.

[20] G. Dalabanjan and N. D. G, "Enabling Attribute-based Access Control for OpenStack Cloud Resources through Smart Contracts," Procedia Computer Science, vol. 233, pp. 861–871, Jan. 2024, doi: 10.1016/j.procs.2024.03.275.

[21] C. Zhang and Y. Xu, "Institutional innovation essence and knowledge innovation goal of intellectual property law in the big data era," Journal of Innovation & Knowledge, vol. 8, no. 4, p. 100417, Oct. 2023, doi: 10.1016/j.jik.2023.100417.

[22] T. M. Ghazal, M. K. Hasan, S. N. H. S. Abdullah, K. A. A. Bakar, and H. Al Hamadi, "Private blockchain-based encryption framework using computational intelligence approach," Egyptian Informatics Journal, vol. 23, no. 4, pp. 69–75, Dec. 2022, doi: 10.1016/j.eij.2022.06.007.

[23] Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukkumarasamy, "Robust integration of blockchain and explainable federated learning for automated credit scoring," Computer Networks, vol. 243, p. 110303, Apr. 2024, doi: 10.1016/j.comnet.2024.110303.

[24] M. Kuliha and S. Verma, "Secure internet of medical things based electronic health records scheme in trust decentralized loop federated learning consensus blockchain," International Journal of Intelligent Networks, vol. 5, pp. 161–174, Jan. 2024, doi: 10.1016/j.ijin.2024.03.001.

[25] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," Cyber Security and Applications, vol. 1, p. 100015, Dec. 2023, doi: 10.1016/j.csa.2023.100015.Authors:

DhanarajuMurala Received B.Tech (IT) degree from JNT University Hyderabad, Telanganaand received M.Tech (SE) from JNT University Hyderabad, Telangana. Currently, He is aresearch scholar at the Department of Computer
Science, GITAM University (Deemed to be University), Visakhapatnam, India. His research interests include Cryptography and network security, Data Security in cloud computing and Software Engineering.

Dr.ThammiReddy Konala,adistinguished academic with aPh.D. in Computer Science from Jawaharlal Nehru Technological University Hyderabad, has made significant contributions to the field of artificial intelligence and machine learning. Currently serving as a Professor and Dean-School of Engineering and Sciences, GD Goenka University, Sohna Road, Gurugram.his expertise spans various technical domains including Java, Python, R, SQL, and data mining. His research interests include blockchain, cyber security, and AI/ML, with numerous publications and successful supervision of Ph.D. scholars.