Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

An Efficient Integrity Controlled CP-ABE(IC-CPABE) for Audio Cloud Block Chain Transactions

Dhanaraju Murala[1], Dr.K.Thammireddy[2]

[1]Research Scholar Department of CSE, GITAM School of Technology, GITAM University, Rushikonda, Visakhapatnam, India. dr1212murala@gmail.com.

[2]Professor Department of CSE, GITAM School of Technology, GITAM University, Rushikonda, Visakhapatnam, India. tkonala@gitam.edu

Article History:

Received: *25-05-2024*

Revised: *06-07-2024*

Accepted: *24-07-2024*

Abstract:

For increasing size of applicants data, in audio-based application, That motivate poor security level of audio data and some time results in invasion our personal data by third party. To fill this loop hole there has no any work on data integrity improvement, Their planning to do a novel framework. In this framework, an optimal data integrity algorithm, Group-wise Attribute Initialization and Policy construction. It would be implicit in each group, in data encoding and decoding by the activation of attribute-based encryption policies. To provide the integrity for audio data, there has a novel hybrid non-linear integrity-based dynamic hashing methodology.Further more, there has a hybrid Ciphertext-Policy Attribute-Based Encryption for data encrypting and decrypting. Next, under ensemble and parallel architecture, the IABE model verification against KABE and TRAK-CPABE. It does a comparative study on encryption and decryption runtimes, on different groups of size, in audio data.The group created from combination of some chosen attribute in IABE scheme, and it's consists of heterogeneous groups and the groups are connected by sub groups of different size. The runtime compare between IABE scheme, classical KABE (Cloudfile_KABE) and TRAK-CPABE (TRAK-CPABE).In encrypted audio data, the hash bit variations is the key parameter, which check as a different identifier and it helps to communicate audio data encoded or it might utilize as security process. The same parameter computed in IABE model, with the existing known model: Cloudfile_KABE_MD5 and TRAK-CPABE_SHA-512 for different group size.The work also works on Hashing technique of transcription audio file, to evaluate memory usage and execution times. It used the real samples of audio bunch like, 'KITCHEN', 'microwave','scream2' and other.The analysis is based on execution time in select different file size, by using directly hash value, It returns different hash value compared with the previously value used. If system again replay any data within the largest hash size.

Keywords: data integrity, group access control, cloud data security, encryption, block-chain.

1. Introduction

The increasing demand to access data remotely requires stronger privacy-preserving and secure algorithms to reduce vulnerability [1]. In the case of audio data, which can be very sensitive in nature, the need for privacy against misuse and unauthorized disclosure of sensitive audio data is of paramount importance to convince stakeholders of discussing freely about particular situations [2].

Unlike traditional storage methods, cloud storage has several advantages for storing audio data, such as ease of accessibility anywhere, anytime and also provides cost-effectiveness depending on use [2]. However, the distributed nature of computing in clouds introduces several prominent security challenges [2]. We know that big data in computers is not necessarily secure. Multi-user sharing of data on a large scale over widespread networks significantly increases the risk of data breaches, tampering and other forms of misuse or unauthorized disclosures [2]. This may lead to reputational loss, information loss and diminished privacy for the authorised users as well as data owners. Existing techniques in data security, such as using smart contracts, access control models, etc, ensure a certain degree of security for data sharing among users, but may not be suitable for very specific features of audio data [3–4]. Secondly, the security of cloud storage persists mostly on the service provider, which can be a potential weak link [3–5]. New cryptographic schemes capable of achieving secure and efficient sharing of audio data in the cloud are explored using the technique of attribute-based encryption (ABE) to address the aforementioned limitations on security and privacy [6]. This approach focuses on maintaining confidentiality as well as integrity of sensitive audio information while retaining the ability to provide fine-grained access control. Future direction of research may include integration with blockchain to ensure tamper-proof storage and management of data.

A new method of the ABE scheme with quadratic residue was proposed based on three main concepts: bilinear pairing, quadratic residues and lattices. It is to afford users a secure mode for both confidentiality and privacy. We made some proposals to offer the efficiency of cost computation and communications as well as the integrity and availability of the data for Cloud computing. We set a remote data possession scheme to realise the integrity and availability of data storage from a service provider under the network environment. Moreover, we also considered the communication cost, and the verification scheme can be conducted under the remote data possession scheme. The cloud users may encounter only a few challenges and their corresponding correct answers, without duplicating the data locally. But there is a limitation on the number of challenges the users may meet in this remote possession scheme. A Provable Data Possession (PDP) scheme has been outlined especially for the restricted capability of mobile devices, especially for mobile cellular users. The computing devices only need to generate their secret keys and random numbers by trust with a TTP. The use of pseudo-random sequence made trouble to this scheme. It will assign a heavy workload and a larger storage space in the mobile devices for more security. The schemes presented in [8] did not give the sufficient security assurance to the cloud users, besides, they would not take into account all data elements while verifying the data integrity. In [9], to afford the cloud data storage with more security and overcome the shortcomings of the above schemes, we presented a homomorphic distributed verification method for proving the integrity of storage data based on the more uniform Sobol sequence over pseudo-random sequence.

The issue of confidentiality is becoming more and more important as a lot of recent growth comes from the cloud computing area. Almost all industries expect to migrate to the cloud at some time. There are two main problems for cloud computing, one is data security when data is stored in cloud and other is data confidentiality. To tackle those challenges, some latest algorithm was developed. Most of them are under the cryptographic functionality and tailored to cloud computing. With those latest method people can resolve the security concerns. Nevertheless no such a good algorithm exist

fully guaranteeing data safety and privacy before the data ran on the cloud server environment. Before storing some sensitive personal information into the cloud server, all of those concerns relating to data safety and confidentiality ought to be properly solved.

Blockchain can work as an autonomous central entity – an intelligent system without direct human and third-party involvement. It will be independent from any attack surface or exploitation. This independence improves the performance and reduces potential bottlenecks and latency layer. All the honest miners (transaction verifiers) in a blockchain network will detect any illegal audio data trade and will not allow it. Once an audio data transaction becomes part of the blockchain, it is very hard to modify or revert back as the information will be cryptographically locked, and very hard to tamper with due to its distributed nature.In the event of any anomalies, audio data transactions can be quickly detected by peers inside the blockchain network who can rapidly identify any discrepancy. Blockchain technology is in its design transparent; hence, there is no way to hide any information. All the nodes will have equal rights to see everything; this can resolve trust and accountability issues. Blockchain technology addresses the problem of securing audio data in the cloud by implementing best-in-breed cryptographic methods. Strong encryption methods will help to keep the data secure and will also help to identify any intrusion attempts and prevent them.Decentralised blockchain design can help to eliminate a single point of failure, which is very important in securing the distributed network. This is a key factor that will help the system to resist sophisticated modern cyber-attacks. The decentralised nature of blockchain by design can help with operational efficiency, meaning it can manage a large number of transactions. Audio data being distributed and travelling to different destinations could involve a large number of transactions.Blockchain can achieve the required performance and scaling capability by using integrity and encryption algorithms and protocols to handle huge loads. When the blockchain network expands, the addressing scheme becomes even more interesting as the system creates a unique, random address for each transaction. Blockchain design is very flexible and elastic, and the system can grow without limits in a similar manner to the internet itself.

2.Related works

Centralised databases can be efficent and reliable, boost productivity and reduce the frustrations of operating teams.(kumar) However, their centralized nature also comes with inherent risks and limitations.(...) [11-12] A decentralised databases never expose all of its information to a single point of failure, which creates vulnerability to a complete loss of data(…), or today, the hum of cloud backups and cloud services.Furthermore, a decentralised databases is a living system, containing data that is spread throughout multiple networked systems wherein each has a uniquely different copy of the database.Overall, various factors ought to inform an organization’s decision of choosing a centralised system or the decentralised one, with the literature echoing steady and faithful lessons about both systems’ strengths and vulnerabilities. It is no surprise that an organization will choose to adopt one or the other depending on its specific needs if not its very raison d’être, the size of its operation, and scale, what information or form of data is intended to be archived or processed, and the balance of such factors as expediency with risk and control.

The DAP allows for a standard and direct payment without involvement of a centralised authority; therefore the parameters of operation like who pays, who is paid, and how much is paid remains confidential and cannot be traced. The assessment can calculate the expenditure of every operation on smart-contract, and it will remain the same for fairly complicated audio tasks. The framework allows for storage and verifies the origin of audio data and it is immutable. It can only be successful if a majority participate sincerely. No one can delete any record that has already been written. How can audio data be securely shared within a network? an architecture of blockchain technology was implemented for each device, it has a chaincode which gets installed and operates as a validating peer of Hyperledger blockchain. The architecture operates on a permissioned blockchain, which makes it a reliable secure framework to maintain privacy and availability of private audio data. [10] proposed an architecture to facilitate audio information sharing. Audio Sharing Architecture allows to facilitates information sharing in a reliable way for health existing public blockchain architecture. This means the transactions that are going to take part will be fast and. The speed and scalability become efficient enough as well because the system designed uses a special transaction protocol that will validate the network activity and it requires only a small fraction of the complete blockchain network.

The aim of this architecture was built to overcome the limitation of a permission-less network which in this case it will lead to the increasing number of untrust nodes especially those that don't intend any transaction which only leads to a network slowdown.

The problem about audio records management is that they are stored in different databases, it becomes very difficult to oversee and they are handled without any validation. The blockchain architecture allows for this. There is obvious evidence of efficiency, adaptability and cost-saving The founders designed a blockchain system to protect their users' privacy. Industry now favour and like carefully considered solutions; many of them will start to favour it.

Because most blockchain projects are open source, researchers around the world are able to join forces, using publicly available code and communicating openly on online discussion boards and audio collaboration tools. This study shows that there is a number of problems with blockchains, but it is heartening to see that developers are taking them seriously and working towards solutions with their own research and development efforts: This study confirmed the problems of secure use noted in the extant literature, and it overcame the problems by using open communication on discussion boards and audio collaboration to explicitly address the users’ concerns about usability issues that they attributed to blockchain-based audio products.They also write: Audio users attribute the security-driven usability concerns that they experience to the aim of blockchains. This might be changing the area of technology. Most audio users were aware of and accurately identified usability problems that can hinder entry into a wide area of technology. These users care about the privacy of their audio data, but they are also aware of the transparency of blockchains. This shows that there are reasons to be careful when claiming that users are not competent, responsible or cognitive enough to make decisions about new technologies. In other words, blockchains are not scalable or efficient.The study, like so many others, also explicitly stresses the importance of presenting clearly and carefully researched results: Even if there is a lot more research and development that needs to happen to bring

blockchain into common use, this study stresses that we will have to be precise in presenting this research.From the second perspective, there are specialist use-cases that could benefit from an alternative solution to the sustainability problem. In a sector such as logistics, which is already facing penetration of blockchain, there is currently a need for greater security of audio data, more stakeholder trust, better traceability and greater decentralisation of work processes. The fact that blockchain technology and smart contracts are evolving and that companies do not need blockchain to become ubiquitous brings opportunities to firms regardless of whether they are wider in society. All nodes that are connected to the network agree on consensus procedure for insertion of new records into the ledger.

Rows of transactions are joined together in linked blocks, handed from one node to the next, in a blockchain system. Peers that make up the network have copies of the full ledger. The building blocks of blockchain technology have been studied:

Block Structure: Transactions are bundled into tamper-proof blocks, ensuring data integrity.

Consensus Mechanisms: These distributed algorithms validate transactions and maintain network agreement.

Digital Signature Cryptography: This technology guarantees the authenticity and non-repudiation of transactions.

Smart Contract Development: Solidity, a programming language, to create tamper-proof smart contracts.

Beyond the technical aspects, studies have explored the impact of blockchain across various industries:

Finance: Streamlining and securing financial processes like payments and asset management.

Supply Chain Management (SCM): through the use of SCM, buyers, sellers and all members of the supply chain can have access to immediate information pertaining to the position of the goods at each stage of the supply chain. Thus, the technology has an inbuilt security and transparency mechanism.

Healthcare: Facilitating secure data exchange and record-keeping for patient information.

The popular image of this is in ‘trustless’ interactions, where ‘trustless’ means that you don’t essentially have to send anyone money and know you will receive the geohash back, or you don’t need to borrow money from a bank. If everything is run by a smart contract, a self-executing agreement, then a third party is no longer necessary because the contracts contain the enforced rules. At this point, we are getting into purely speculative territory; but, again, new kinds of audio use cases would be enabled by the further research and development work that is needed.

Yet blockchain technology itself as posing all kinds of network participation, consensus protocols and shared ledger maintenance issues both in public and private networks. Smart contracts too, especially within the business context, are difficult to implement because of the technical complexity of blockchain and the difficulty of its usability. Researchers have established models for

technological adoption of e-governance: some of these models use the fit-viability model and others use the diffusion of innovation theory in the setting of smart government. Security considerations imbued within each theory aid in modelling and design for technology so as to ensure a compass of reliability and accuracy within data extraction and adaption. Ability features such as public – private dichotomy, public real-time immutability integrity and hierarchical complexity were identified as an ideal setting for smart contracts while other ability features like binding key generation, secure private information management, data redundancy, collusion resistance, independence and localised update were equally important.

Multiple Levels of Encryption for Robust Data Protection

One way to protect data is to use two laterers of encryption. The owner of the data first encrypts it to get the first layer of protection, and then the server adds a second layer of encryption that allows the policy to be changed as needed. In this manner, the system balances the tension between security and policy flexibility. Whenever there's a major policy shift, a new policy development process is used to emphasise essential features and preserve data confidentiality.

Tools for Managing Access and Attributes

Second, it can use a group key server to build and distribute shared keys to groups, so that users can access data according to their group memberships. Third, we design a special purpose tool to help data owners reason about attributes and policies relating to users' access the owner's data. It helps determine who the potential initial data subjects are, by checking whether subjects are compliant with policies and possess the required attributes.

Advanced Cryptographic Techniques and Privacy Enhancements

Some researchers have experimented on enhancing the security by storing only the hashes of the data, or linking those hashes using advanced cryptography. We should also mention a very promising approach that combines the new field of homomorphic encryption with query processing in secure settings and differential privacy, which guarantees degrees of anonymisation of the data.

Blockchain for Decentralized Data Control

They also used blockchain as a secure data store and access-management system ([12]). Experiments with proxy re-encryption allow for the creation of such compact encrypted documents with an associated key management system. Smart contracts may also be coded to control user access to the system and invite third parties via the blockchain network, leading to a more distributed system with more control.

Smart Contracts and Cryptographic Techniques for Audio Data Consent

A blockchain solution geared for audio data consent was developed (13). It simplifies user consent management by utilising smart contracts and provides tools to data consumers allowing them to have control as well. Furthermore, this method incorporates homomorphic encryption to query over audio data and differential privacy for anonymising audio. Blockchain is used to secure storage of these records in cloud infrastructure.

One method leverages blockchain techniques for secure audio data exchange ([14]). It could enhance a dynamic consent method, citing Access Matrix (ADA-M) and Data Use Ontology (DUO) to minimize the risk of audio data leakage, simultaneously leveraging Fabric blockchain to conduct authorization verification and reduce the decryption burden on resource-constrained IoT devices. Meanwhile, smart contracts on the blockchain are used to deal with the complexity of decryption in "High-complexity partial decryption", reduce the user burden abovementioned.

Besides, it also applies blockchain techniques to scaffold historical data traceability simultaneously with data limitation based on security. Meanwhile, the system realizes overall performance enhancement through its quantitative evaluation in a hierarchical attribute-based cryptographic model.

AuthPrivacyChain: A Blockchain-based Access Control Solution

The other one, a blockchain-based access control architecture with privacy–protection designed by [15] (hereafter referred to as AuthPrivacyChain), was first using to adopt node account addresses, but because of the distinct features of the data in the blockchain, it evolved toward data encryption and access control models of permission granting and revocation. Notable of this model is the way it utilises the controls EOS provides to manifest the privacy measures. This model encrypts and stores the access control permissions in the blockchain, ensuring that only valid users can access certain data. The blockchain also makes the system accountable for the resource usage and guarantees data integrity, being impervious to internal and external attacks.

One algorithm, for example, ensures data privacy in smart-city apps such as PrivySharing (yes, that is the name), confirming with all parties to such smart-contracts the protection of user’s data. Additionally, complying with the EU General Data Protection Regulation (EU GDPR) which emphasises user privacy (such as the right of access, transfer and erasure).

Leveraging Audio Data for Enhanced Accessibility

This approach calls for collections of audio recordings that are organised together with lab results, sensitive data and other documentation, and that can enable greater accessibility, accuracy and efficiency than previously possible.

Multi-Layered Security for Data Protection

Photo for representational purposes If adopted, this protocol would provide a holistic approach to data protections through a layered protection made up three well-established cryptographic methods – Diffie-Hellman key exchange; Advanced Encryption Standard (AES); and another key exchange method such as Hellman.

Many experiments have been proposed to secure the data in a cloud storage setup. These include:Encryption of data: the Diffie-Hellman key exchange is used for key confidentiality and secure data transfer. It prevents the hacker and the database server to have access to the stored data [17].Saving cloud data: many experiments are being conducted on saving the cloud data through modern encryption standards, file distribution and SHA1 hashing algorithm [18]Server-based data

distribution: Server-based distribution becomes a security concern. But, hash-code file can be saved for an authenticating user. It reduces the mess and specification. This method can be used to solve data integrity problem, error localisation and security consideration in a single package [16]. Therefore, this system can effectively prevent server collusion, tampering with data repositories and altering data.Securing the cloud storage servers: Many experiments [19] are being deployed to secure the cloud storage servers. A novel approach for: server security is based on proxy re-encryption combined with a standard data encryption method, for example the Advanced Encryption Standard (AES) algorithm. Till now, proxies have been necessary for data re-encryption on each link, which causes multiple operations and therefore increased memory usage and processing time. PRE has been designed such that it replaces a proxy on each encryption link and, consequently, replaces the memory-intensive proxy with a single re-encryption operation. Our system employs the proxy re-encryption and erasure coding techniques. The first part uses PRE to encrypt the information that can be stored in the cloud, whereas the second part makes use of distributed erasure coding, a type of data storage. Since PRE works only with block ciphers, we have employed AES. Combination of proxy re-encryption and erasure coding realises the secure storage and sharing of information in the Cloud, in a way that block ciphering encryption/decryption algorithms avoid tampering with the data [19].Erasure coding encodes the data, where in if a file becomes damaged or destroyed, only a few components remain intact to recover the whole data. This also reduces data authorisation within the system where data blocks represented as matrix are distributed within decentralised system.

This result shows that the computational cost of this scheme is lower than GSW and DM schemes for depth-2 binary (NAND) circuits and sufficiently small error rate.

In this paper, they research and optimise an all-in-one binary homomorphic encryption scheme. If all data stored in the cloud have no control of you, that data is not trustworthy. Data privacy and data leakage is big concern for cloud security. Based on network defense, the authors propose a secure approach on cloud.

Traditional cloudproof encryption schemes store the stored data in ciphertext, and if computation is needed, it needs to decrypt the ciphertext to the plaintext and perform computation, which causes a certain privacy risk. The study propose homomorphic encryption, which is able to perform ciphertext operations, without leaking the given data. When a third-party user loads and processes the ciphertexts, he/she does not need to trust the cloud.

The study also tackles the difficulty of large multiplication for fully featured homomorphic encryption. The researchers propose an optimal operand reduction scheme that can reduce the area overhead for radix-r butterfly units by 25 percent. An experimental result infers that the optimisation method can achieve area and time reduction of 69 times and 1.177 times, respectively. Compared with other related works, the proposed design is more efficient in terms of area and processing time. The authors also design an AES (Advanced Encryption Standard) processor for efficient cryptography that achieve high throughput and low area congestion.

3. Proposed Model

We present a new data security framework for integrating cloud blockchains into secure applications and specifically present an audio data cloud integrity protocol. We outline its key features below.

RBAC: Role-based access control, where users are granted access rights and roles based on their organisational function.

Group Attributes as Integrity Checks: Each group's attributes constitute integrity checks and access policies are dictated by these attributes.

Enhanced Integrity Algorithm: A Non-linear dynamic Algorithm for integrity (MAC) replaces hashing (MD5, SHA, and Whirlpool) in the block creation process.(Figure 1: Overall Framework)

This framework addresses limitations of traditional models:

Independent Encoding/Decoding: Unlike traditional models, this framework integrates group-wise data encoding and decoding.

Blockchain Security: Every transaction involving audio data undergoes a blockchain security mechanism. This involves hashing and encrypting the input transaction with security blocks, strengthening the overall blockchain security. Additionally, current and prior block hashes are encoded for added robustness. (Figure 1 showcases these security features)

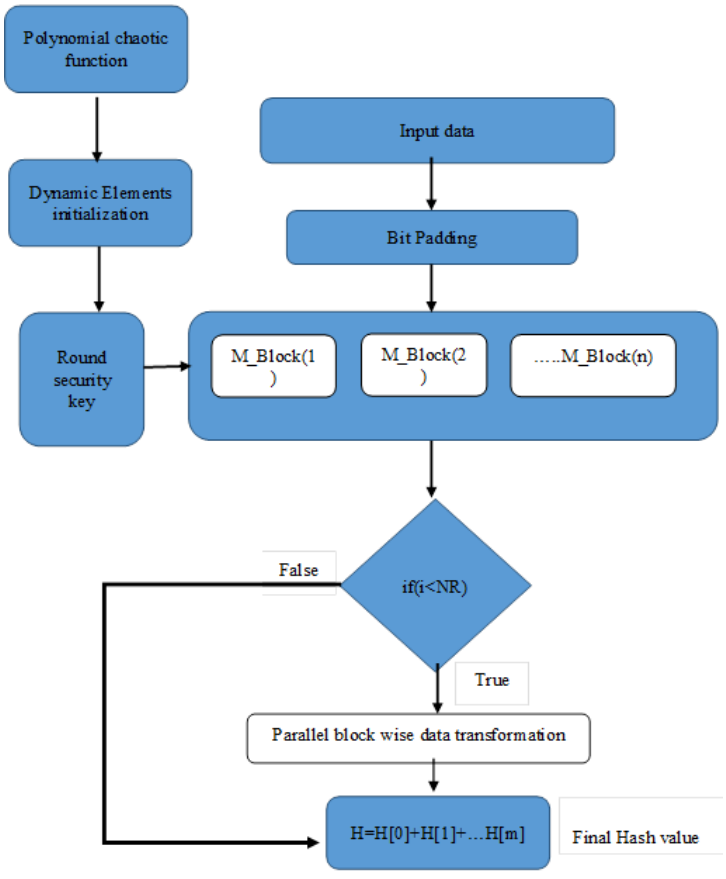


Figure 1: Proposed block-wise chaotic integrity model

Attribute-Based Encryption (CP-ABE): The framework utilizes CP-ABE, offering greater flexibility compared to KP-ABE (Key-Policy Attribute-Based Encryption). Users can choose individual attributes or combine them from a provided set for access control (as depicted in Figure 1).

Here's a step-by-step breakdown of the proposed framework:

Step 1: Group-Wise Attribute Initialization

An optimal integrity algorithm employing a strong hash function is used to initialize group attributes. This ensures data integrity and security.

Group attributes are generated for a CP-ABE scheme, enabling secure and attribute-based access control.

Step 2: File Grouping

A compression function efficiently groups files together, reducing their size and optimizing storage within the cloud environment.

Step 3: Policy Definition for Each Group

For each group of files and each group of attributes, the framework defines access policies. Each assertion has the form: ^(attribution, integrity value)+ Schematically, these policies define the conditions that must be satisfied for access to the files in each group. The group of attributes was (after the files and the data have been ‘deleted’) hidden by setting the integrity value to NaN (‘not a number’) The attributes of each group of files are used to enforce access control.

Step 4: Encoding and Storage in Cloud Storage

Then, each group of files is encoded (for example, by encrypting the data) before it is saved into the cloud storage. The metadata (the information of which files are stored) and the encoded data (the compressed group of files) are stored with high confidentiality and integrity.

Step 5: Authorized Data Access and Decryption

An authorised user can extract the stored data provided she knows the proper cipher text, and also satisfies the associated access policy. In this case, the system decrypts the data such that the file is made available to the authorised user for recovery.

Ensuring Audio Data Integrity at the Group Level

This system has a new hybrid Random Heterogeneous homomorphic integrity check mechanism to guarantee that audio data in a group are safe. The mechanism generates a newly generated hash value at the encoding and the decoding process. The principle of such mechanism is non-linear mathematical transformations that is used as an algorithm (shown in figure1) .

Figure1 - the basic principle of the linear algorithm

Step 1: Initialization cloud input data C_M .

M_B=Bytes(C_M)

Polynomial chaotic key initialization :

Let P be the chaotic polynomial function with the following recurrence relations.

$P_n(x) = \alpha P_{n-1}(x) - \beta P_{n-2}(x)$; where α, β are the random number.

Let P_n be the set of nth polynomial box with N functions.

$$P_0(x) = k,$$
$$P_1(x) = kv \quad -$$

$$P_n(x) = \alpha P_{n-1}(x) - \beta P_{n-2}(x)$$

Initialize the dynamic secret elements using the $P_n(x)$ function as D_{sk} .

$$D_{sk} = \{\delta_1, \delta_2, \delta_3, \delta_4\}$$

The polynomial random value is generated using the nth derivative of P_n as

Rn[i]= $D(P_n)$ // where D is the nth derivative w.r.t x.

Step 2: Divide cloud message M_B into k blocks as B[k] of length 32bits(4bytes).

Step 3: Padding input message if the length exceed the block size with 0000001

Step 4: For each k-block

PoiVariate $\eta(x = 1, \lambda = 0.5) = e^{-\lambda}.\lambda^x / x!$
$DLN[] = LogNormal(\eta.\mu, \eta.\sigma);$
$DBox[] = \{DLN.mean, DLN.Variance, DLN.Kurtosis, DLN.Skewness\};$
Generate Dynamic Round key as
$\phi 1 = RK[] = DBox[r];$
Get Q and R matrices using GramSchmidt QR decomposing.
$CauPoly(x) = |p\_n|x \wedge n + |p\_\{n-1\}|x \wedge \{n-1\} + ... + |p\_1|x - |p\_0| = 0$

CharacteristicPolynomial Equation is constructed using the
R decomposion matrix as CP.
EigenValues EV[]=CP.getEigenvalues();
Rk=Rank(Q)
GaussianFunction $GF(a,b,c)=a.\exp(-(x-b)^2 / 2.c^2)$
$M\_RK[] = \{EV[0], CauPoly.lb, R, GF(R\,k, RK[0], RK[1], RK[2]\}$
$\alpha = \lambda * \exp(\lambda * B[k])$
$\beta = B[k] \bmod(\alpha)$
$\phi 2 = M\_RK / \sqrt[3]{\alpha * \beta}$
Integrity $I[]=\phi 1 \wedge \phi 2 \wedge B[k]$
done

Step 5: Final Hash $H[i] = I[0] \,|\, I[1] \,||\, I[2] .. I[n]$

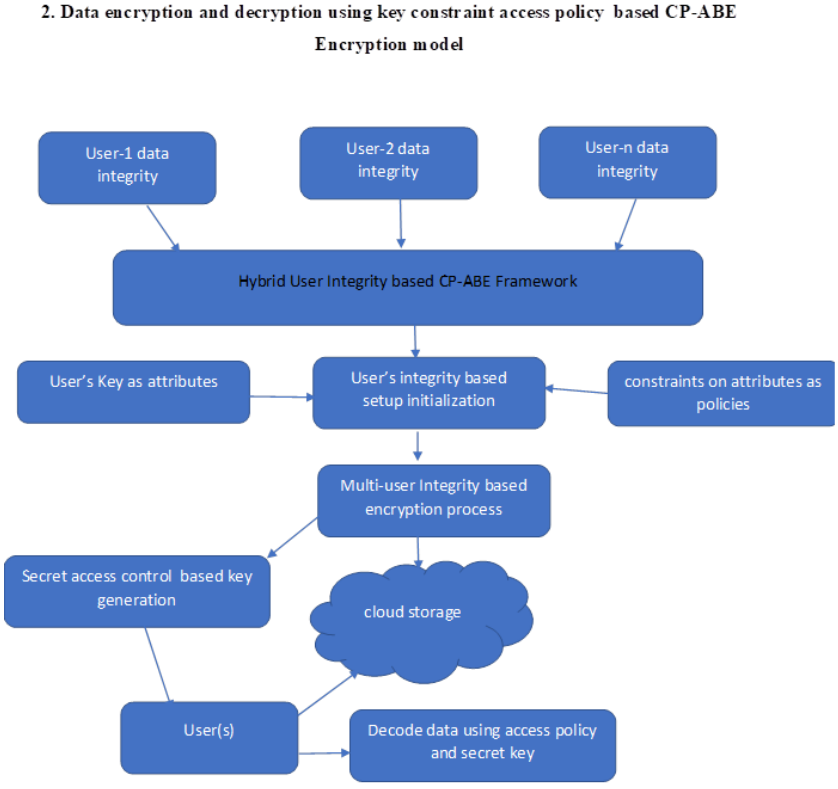


Figure 2: Data encryption and decryption using key constraint access policy based CP-ABE Encryption model

The purpose of the model is to provide a multi-user non-linear proof integrity based encoding model in an audio data stored in cloud. According to the figure 2 below, the model provides 4 key phases model in the block chain encryption Technology Counted as, (i)Multi-Access groupwise Data

Encryption Phase, (ii)Multi-Access groupwise Audio Data Encryption Phase, (iii)Multi-Access groupwise Secret Key Generation Phase, and multiple group wise Data Decryption Phase.

However, as a concept/technique, ABE is a highpotential field to deal with the important and widespread problem of confidentiality-preserving data sharing, particularly in distributed cloudcomputing environments. The basic idea of using ABE for data-sharing systems is to grant access to data blocks based on the attributes held by a set of users. Below, you can find an updated description of a Multi-Authority ABE (MA-ABE) implementation for a multi-user cloud environment.

Phase 1: Setup and Key Generation

These policies will define who will have access to what, and to whom the data will belong. Policy Definition: Users and their access privileges are defined. The access policies elucidate what users have access to.

Randomised Hashing: Generate the key by hashing an unrelated value through a 'hash function' At the application layer, keys might also be inferred using randomised hashing which adds a layer of security - in this case by making the keys less predictable.

Cryptography: Key generation This step relies on bilinear pairing elements and exponents in cyclic groups. Cryptography: Encryption This step simplifies encryption and decryption processes.

```
function GeoDist(x, p)
    return x * (1 - x) ^ p
end function
function UniDist(m, d1, d2)
    if d1 <= m <= d2 then
        return m / (d1 - d2)
    else
        raise Error("m not in range [d1, d2]")
    end if
end function
# Initialize cyclic group elements for multi-user access control
Zr = initializeCyclicGroupElement()
G1 = initializeCyclicGroupElement()
G2 = initializeCyclicGroupElement()
# Define bilinear_map function
function bilinear_map(groupElement, mappingFunction)
end function
# Define functions or variables for GeoDist and UniDist
mu_GeoDist_x = defineFunctionOrVariable()
mu_UniDist_x = defineFunctionOrVariable()
sigma_GeoDist_x = defineFunctionOrVariable()
sigma_UniDist_x = defineFunctionOrVariable()
```

# Calculate alpha using bilinear map
alpha = bilinear_map(Zr, mu_GeoDist_x)
G1, G2: Likely cyclic groups used in the bilinear pairing construction.
bilinear_map: A mathematical function essential for the pairing-based encryption scheme.
mu_∞, mu_ω, sigma : Parameters related to data distribution (presumably uniform and geometric distributions).
Z_s: Presumably a finite field.
g, h, gp, g_α, β: Elements within the groups.
Equations with Explanations
Calculating Mult_PubK(g):
Mult_PubK(g) = bilinear_map(G1, max(mu_∞ * UniDist(x), mu_ω * GeoDist(x)))
Seems to compute a public key element based on a combination of data distributions and group G1.
Calculating Mult_PubK(gp):
Mult_PubK(gp) = bilinear_map(G2, sigma * GeoDist(x))
Likely computes another public key component using a geometric distribution and group G2.
Calculating Mult_MasK(beta):
Mult_MasK(beta) = bilinear_map(G2, sigma * UniDist(x))
Seems to generate a master key component using a uniform distribution and group G2.
Calculating Other Multi-User Key Components:
These equations appear to perform a series of bilinear map calculations to generate multi-user public and master key elements. They likely involve chaining previously calculated values and raising elements to the power of Z_s.
Multi-User Public Key:
Multi_User_PublicKey = {g, α, Mult_PubK(g), Mult_PubK(gp), Mult_PubK(h), Mult_PubK(g_α)}
Lists the elements comprising the final multi-user public key.
Multi-User Master Key:
Multi_User_MasterKey = {Multi_MasK(β), Multi_MasK(g_α)}
Lists the elements comprising the final multi-user master key.

Public Key and Master Key:

Multi_User_PublicKey: This defines the public key information for multiple users. It includes elements like g (a generator of a group), α (potentially a system parameter), Mult_PubK(g), Mult_PubK(gp) (possibly related to the public key of a global parameter), Mult_PubK(h), and Mult_PubK(g_α). These components, likely along with additional information not shown here, form the complete public key.

Multi_User_MasterKey: This defines the master key information. It includes the multi-masked versions of β and g_α. The master key is used by the authority to generate user secret keys.

Phase2:

Attribute and Policy Setup: The system establishes the attributes associated with users and defines integrity-based access policies. These attributes and policies will later control who can access the encrypted data.

Data Encryption with Access Tree: The data is encrypted using a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. An access tree structure is embedded in the ciphertext, representing the policy that must be satisfied for decryption.

Sets:

A: Set of attributes

P: Set of integrity policies

Zr, m, Zn: Cyclic groups

Public Key: PubK

Cyclic Group Parameters: α, β (relatively prime to the multiplicative group)

Security Metrics: C1, C2 (computed using unspecified equations (1) and (2))

cloud_ins_id: Cloud instance ID

cloud_ins_name: Cloud instance name

r1, r2, ...: Randomized cyclic pairing elements

A1, A2, ...: Multi-user identities as attributes

P1, P2, ...: User integrity values as policies

Computations:

C1 = hash4096(cloud_ins_id)

C2 = hash4096(cloud_ins_name)

CP-ABE encryption using access tree T (constructed from P), attributes, policies, and randomized pairing elements

Encrypted cloud user data

Security metrics C1 and C2

Key Assumptions:

Ciphertext generation in the Initialization Phase follows a standard model (not specified).

CP-ABE encryption process aligns with a conventional CP-ABE scheme.

Equations (1) and (2) for C1 and C2 are based on cryptographic hash functions and potentially other security measures .

Phase 3:

Muli-user data access control based key generation:

Multi-user Data Access Control Based Key Generation

This approach generates keys by combining user attributes, integrity values, and a master key to create complex private keys that manage access to encrypted data.

Key Elements:

H_Attlist: A 4096-bit value representing the user's integrity. This value likely helps ensure that only authorized users can generate the correct keys to decrypt data.

G1, G2: Cyclic groups, which are mathematical structures used in cryptography because their properties make them suitable for key generation and encryption.

r, g_r, g_p, r_j: Random generators within the cyclic groups. In cryptography, randomness is essential for making keys unpredictable.

Cauchy Distribution (CD(d)): A probability distribution that may be used to introduce randomness or noise into the key generation process.

SecrK.Dj: Likely represents a portion of the secret key associated with an individual user or data segment. The calculations suggest it is derived from the user's integrity value (H_Attlist) and random elements.

PK.gp.powZn(r_j): Appears to be a power computation within a group, possibly related to public-key cryptography. Here, 'PK' might refer to a public key.

SecretKey: The final secret key seems to be a collection of elements derived from the Cauchy distribution, attribute information (SecK.attr, Attlist), and the calculated SecrK.Dj values.

Multi-user Dynamic Encrypted Data: In this phase, a dynamic DK[] are taken as input from the cloud users for data decryption process.

4. Experimental results

The work involved comprehensive experimental evaluations conducted on a real-time cloud server within a Java environment. Setup:

Real-World Testing: The proposed system was evaluated on a live cloud server (Amazon AWS) within a Java development environment.

Blockchain Integration: A blockchain framework was implemented for additional security measures.

Tools: Third-party libraries (Apache Math, JAMA, Java Pairing, AWS JDK) were used to support data integrity and security calculations.

Metrics:

Hash Bit Change: Measures how many bits within the data hash change due to alterations in the original data. This is crucial for ensuring integrity and detecting tampering attempts.

Encryption/Decryption Runtimes: Time taken to encrypt and decrypt data (measured in milliseconds). These metrics assess the performance efficiency of the proposed encryption methods.

Cloud Encryption Runtime: Time specifically required for cloud-based encryption, highlighting any overhead compared to local encryption.

Comparative Analysis

The proposed encryption model was compared against:

Integrity Algorithms: Established hashing algorithms (SHA, MD5, Whirlpool, Parallel Chaotic Hash) to provide a benchmark for integrity protection.

Encryption Models: Various Attribute-Based Encryption (ABE) techniques (KP-ABE, CP-ABE, Fuzzy CP-ABE, HCP-ABE) to demonstrate the effectiveness of the new model in real-world use cases.

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

CP-ABE offers fine-grained access control based on user attributes. In the context of integrity, this means that only users with specific attributes (as defined by the access policy) can decrypt the data and verify its integrity.

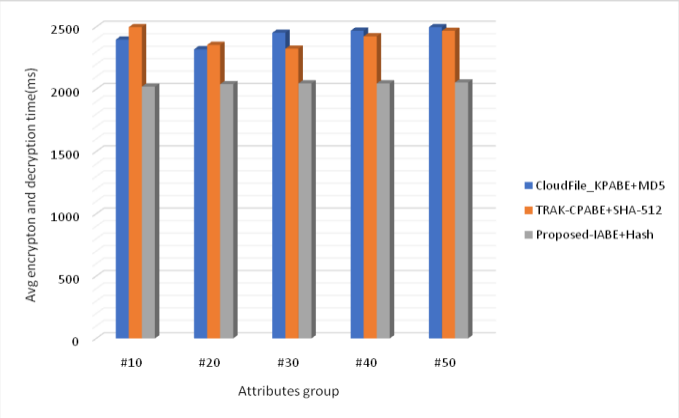


Figure 3: Performance Analysis of the Proposed IABE Model

Figure 3 provides a comparative analysis of the proposed Improved Attribute-Based Encryption (IABE) model against traditional encryption approaches (Cloudfile_KABE and TRAK-CPABE). The analysis specifically focuses on average encryption and decryption runtimes (measured in milliseconds) for audio data across various group sizes.

Table 1: Encryption and Decryption Efficiency

Group No	CloudFile_KPABE	TRAK-CPABE	Proposed-IABE
10	2421	2327	2024
20	2441	2499	2012
30	2375	2396	2101
40	2493	2425	2045
50	2483	2492	2002

This table illustrates the averages of the time needed to encrypt and decrypt with the proposed IABE (Improved Attribute-Based Encryption) model and with traditional methods such as Cloudfile_KABE and TRAK-CPABE by audio data. The main focus is on the runtime of the encryption and decryption process in milliseconds for different group sizes.

Results shown below depict that the proposed IABE model had shorter encryption and decryption times in both methods compared to traditional methods for all group sizes.

(Note: In the IABE scheme, the groups are partially determined by the attribute subsets.)

Table 2: Data Integrity Assessment

Group No	CloudFile_KPABE+MD5	TRAK-CPABE+SHA-512	Proposed-IABE
10	112	114	132
20	113	113	131
30	109	116	138
40	114	115	130
50	114	117	131

Table 2 presents the average bit change for audio data across different group sizes.

Rows: Each row represents a specific group size used in the IABE scheme.

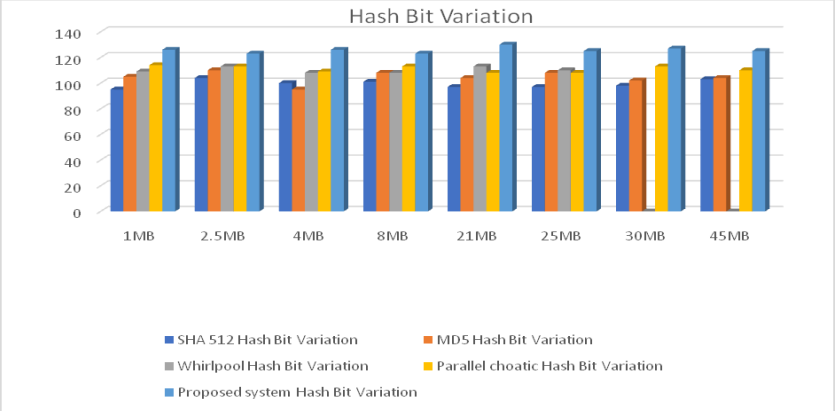
Columns: Each column represents a different approach: CloudFile_KPABE+MD5, TRAK-CPABE+SHA-512, and the Proposed IABE model.

Columns: Each cell displays the median bit changes recorded when one of the tested methods is applied against a certain grouping on the y-axis. The greater the bit change, the more distinct the hash of the altered source data appears from the original, suggesting modifications could have been instituted.

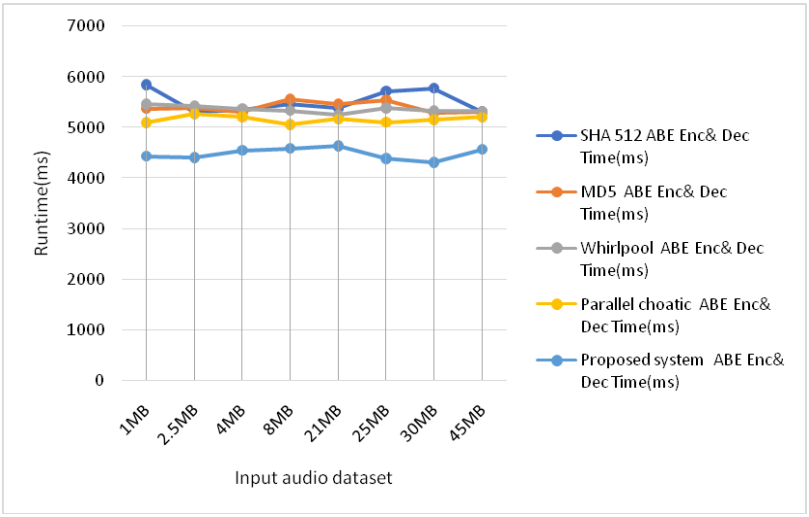
Hashing Technique	**1MB**	**2.5MB**	**4MB**	**8MB**	**21MB**	**25MB**	**30MB**	**45MB**
SHA 512 Hash Bit Variation	95	104	100	101	97	97	98	103
MD5 Hash Bit Variation	105	110	95	108	104	108	102	104
Whirlpool Hash Bit Variation	102	102	109	103	107	103	108	103
Parallel chaotic Hash Bit Variation	114	113	109	113	108	108	113	110
Proposed system Hash Bit Variation	126	123	126	123	130	125	127	125

The given figure compares the hash bit variance between the given 5 hash functions applied on 6 different input files of differing sizes. The Hash Bit Variance is the number of unique bits in the hash values for different input files of the same size. Normally it is expected that higher Hash Bit variance should be there if the hash function is more sensitive to changes in the data.It can be clearly seen that the proposed system shows higher hash bit variance compared to all the existing methods.The graph demonstrates the hashing techniques (SHA-512, MD5, Whirlpool, Parallel Chaotic, and Proposed

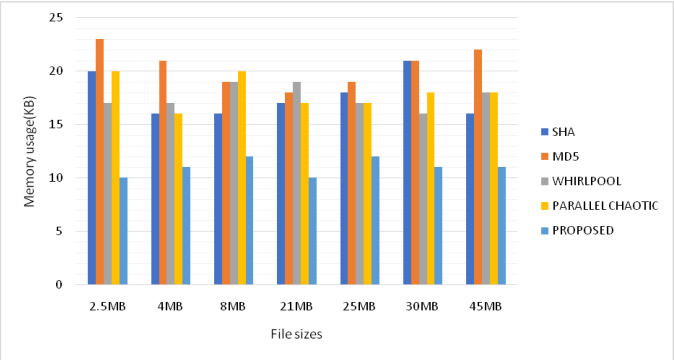
System) comparing the hash bit variance using 6 different input files. The hash bit is the number of different bits created in the hash values for different input files of the same size.It is normal that the higher the hash bit variance, the more sensitive the hash is to changes in the data. We can clearly see that the proposed system has a higher hash bit variance compared to the other existing methods.



The figure demonstrates changes in the hash bit in different hashing techniques ;namely, in SHA-512, MD5, Whirlpool. in Parallel Chaotic hashing technique and also two types of the proposed system(PS1 and PS2) when is applied to input files of 1MB, 2.5MB, 4MB, 8MB,21MB, 25MB, 30MB and 45MB respectively. Hash bit variation is showcases the number of different bits in produced hash value from different files of the same sizes.



The given figure depicts the timing (in milliseconds) of some hashing algorithms (SHA-512, MD5, Whirlpool, Parallel Chaotic and Proposed System) for the cryptographic operations (encrypt and decrypt) of the documents with different sizes(1 MB, 2.5 MB, 4 MB, 8 MB, 21 MB, 25 MB, 30 MB and 45 MB) that were encrypted by Attribute Based Encryption(ABE).Overall it can be seen that the Encrypt and decrypt operation with the Proposed hashing system take less time than other methods. So we can say that using Proposed System gives better performance in term of speed of the cryptographic operation in ABE than other methods.



The figure shows, comparatively, five hashing models : SHA, MD5, Whirlpool, Parallel Chaotic, Proposed and the memory used by each hashing model when large files are processed (2.5MB, 4MB, 8MB, 21MB, 25MB, 30MB, and 45MB) .

Overall, it seems that the Proposed hashing model requires the minimum levels memory usage out of all the other hashing models under test when large files are processed.

On one hand, SHA, MD5, Whirlpool, and Parallel Chaotic require different levels of memory usage to process large files. Between those four, the memory usage allot for SHA and MD5 in comparison with Whirlpool and Parallel Chaotic models.

Realtime Dataset:

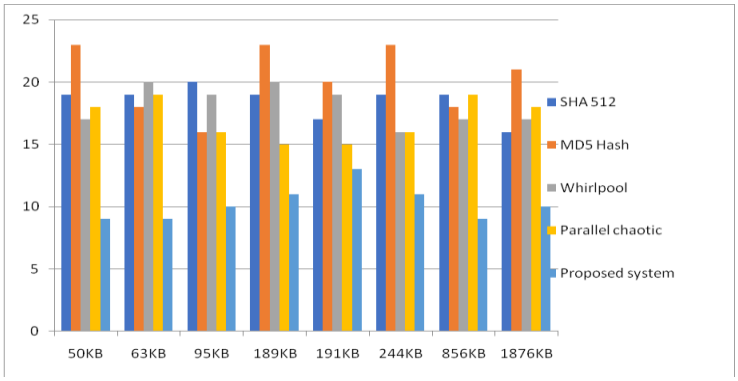
size	**50KB**	**63KB**	**95KB**	**189KB**	**191KB**	**244KB**	**856KB**	**1876KB**
filename	KITCHEN	microwave	scream2	metro	comedy	cheer	market	indian song

Size: This column stands for the size value of the file, expressed in KB (kilobytes) .

Data field and its values: 50KB, 63KB, 95KB, 189KB, 191KB, 244KB , 856KB, and 1876KB .These values represent how much memory or storage of any file that could be used in an environment.

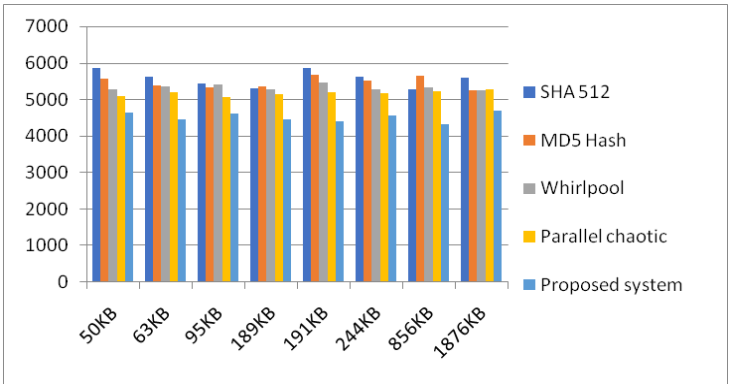
Filename: This column gives us filenames for data files or identifiers for their contents. A data file is something stored, whether that be in an audio format or anything else. These are the names found in the dataset: KITCHEN. microwave. scream2. metro. comedy. cheer. market. indian song. It could refer to audio files of different varieties, processed for different applications.

Memory usage:



The given figure depicts memory usage in kilobytes (KB) as a function of the kind of hashing techniques applied on the live-time audio signal. Each row shows different kind of hash algorithm, while columns indicate different number of samples or scenario involving audio data. The values present the computer memory usage in kilobytes required by the set of prespecified sound data by every hash function technique. For example using SHA512 technique on the prespecified sound sample number 1 takes approximately 50 KB. As we move across the horizontal axis to column 2 we see the required memory usage for the second audio data sample which corresponds to 75 KB. The same pattern/trend is valid for other hashing techniques which have been listed in x-axis. These memory usage values is helpful to identifying the resource requirements for each hash technique as it allows assessing which one is suitable considering the memory resources and real-time performance in live-audio signal processing applications.

Execution time(ms):



The table displays encryption as well as decryption times, given in milliseconds (ms), for three hashing methods and for three file sizes, specified in kilobytes (KB). This inforation is important for the understanding of the performance characteristics of these hashing methods, once applied to the real world.

50KB, 63KB, 95KB, 189KB, 191KB, 244KB, 856KB, 1876KB: The given information is in KB or kilobytes. For each column, the total spent time (in milliseconds) is given by the hashing technique to encrypt (or hashed) and decrypt (or verify) the data of the respective sizes that mentioned in the row.

For instance, 5871 ms has been spent in SHA 512 row for 50KB, besides this time, the verification takes the same amount of time as the encryption. The figure provides useful information for users to decide which hashing method to use for different file size with respect to computational efficiency. The figure includes 11 hashing methods with different results when applied to file size of 2^8, 2^16, and 2^25 bits. From the next figure, overall, lower times would be preferred to faster hashing and verifying from data while higher times would acceptable in applications prefer strong cryptographic security.

Hash bit variation:

Hashing Technique	50KB	63KB	95KB	189KB	191KB	244KB	856KB	1876KB
SHA 512	99	109	101	96	101	98	106	109
MD5 Hash	99	102	105	100	96	108	106	108
Whirlpool	107	100	101	108	106	105	106	109
Parallel chaotic	111	107	111	107	115	107	107	114
Proposed system	130	129	123	130	125	127	130	124

The table illustrates the number of hash bits that vary for various method of hashing, and for represented file size in kilobytes (KB). Hash bit variation will be the number of bits that will change (or will differ) in hash value output, if the same hashing method will be applied for the same data file size but with different data samples.

Hashing Technique: This column lists the various hashing techniques being compared.

63 95 189 191 244 856 1876

Column 50KB 63KB 95KB 189KB 191KB 244KB 856KB 1876KB

SHA 256 93 105 97 78 90 84 87 73

SHA 512 97 98 98 75 92 78 86 74

Blake2b 91 94 85 7 91 78 67 60

SM3 82 80 77 89 85 94 84 64

RIPEMD-320 97 99 93 96 96 85 66 50

CRC32 133 136 150 144 139 134 132 155

MD5 94 97 89 89 92 86 66 62

While these columns indicate hash bit variation for different hashing techniques when applied to data of size specified in the title for the column, the values within these columns carry a message that is quite interesting. Looking at the column with file size 50KB, the value in the "SHA 512" row indicates that the SHA-512 hash outputs are more consistent for data of size 50KB. Precisely, this means that if two samples of data, each of size 50KB, are hashed using SHA-512, the probability of their hash outputs coinciding is p = 1 - 99/1024 = 95.15 percent. Lower hash bit variation values suggest that hash outputs are more similar (i.e, they seldom differ) which, in turn, results in hash bit patterns that are more reproducible on repeated applications of hashing (i.e., if identical data were to result in the same hash, that would be a desirable characteristic for applications where such a requirement exists); on the other hand, higher variation values suggest that hash outputs are more distinct (they exhibit more differences) among samples of different data, which can be beneficial for applications where data particularly needs to maintain its uniqueness, or where it must undergo a highly robust hashing to claim the utmost level of security.

5. Conclusion

In this paper, we propose an improved data security framework for blockchain-based audio applications. The procedure includes: Group-wise attributes initialization with optimal integrity algorithm;Assignment of file groups and compression functions;Access control policy setting;Ciphertext group IDs generation;Encryption and encoding for group ID with cipher text;Save in cloud storage systems; Decoding data with ciphertext and access policies.ABE applied to Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme can support flexible and secure data sharing on the decentralized blockchain networks. However, it has the disadvantage of having too heavy computation overhead and too strict access control policy. In our prototype, we also implement ABE scenario to build our framework. We adopt the improved ciphertext-policy ABE (ICP-ABE) scheme that combines the properties of CP-ABE and IBE (Identity-Based Encryption) schemes which can provide the desired properties of both CP-ABE and IBE. With ICP-ABE, we can design the access control policies to restrict the capability of the person to retrieve the ciphertext. ABE is a popular track in cryptography with applications like distributed storage. It provides flexible security, i.e. the corresponding access control policy defining the people who have access to the corresponding data may have more than one conditions. The advantages of ABE that it uses public-key ciphers to encrypt and decrypt without the requirement of the sending and receiving user exchange a publicly known key. In addition, this feature indicates ICP-ABE has more flexibility style than CP-ABE and IBE separately. A motivation for our framework is to provide flexible and secure data access control for group audio data in a blockchain-based audio platform. With the framework, we effectively resolve the issues of verifying the integrity of the group audio data and managing the variable-sized data while providing flexible and secure data access control of the audio data among the group members in a cloudspace. At the same time, there are some implications and benefits brought to the security, confidentiality and integrity of the audio. In a way, it supports the development of more reliable and secure audio broadcast and audio search in the cloud context. Results obtained in this research have potential and bring advances to the security of the audio in the cloud context.

References

[1] A. I. Taloba et al., “A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare,” Alexandria Engineering Journal, vol. 65, pp. 263–274, Feb. 2023, doi: 10.1016/j.aej.2022.09.031.

[2] Z. Wang et al., “A covert channel over blockchain based on label tree without long waiting times,” Computer Networks, vol. 232, p. 109843, Aug. 2023, doi: 10.1016/j.comnet.2023.109843.

[3] Y. Liu, L. Pan, and S. Chen, “A hierarchical blockchain-enabled security-threat assessment architecture for IoV,” Digital Communications and Networks, Feb. 2023, doi: 10.1016/j.dcan.2022.12.019.

[4] S. Upahm Abas, F. Duran, and A. Tekerek, “A Raspberry Pi based blockchain application on IoT security,” Expert Systems with Applications, vol. 229, p. 120486, Nov. 2023, doi: 10.1016/j.eswa.2023.120486.

[5] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, “A secured distributed detection system based on IPFS and blockchain for industrial image and video data security,” Journal of Parallel and Distributed Computing, vol. 152, pp. 128–143, Jun. 2021, doi: 10.1016/j.jpdc.2021.02.022.

[6] N. Y.-R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, “A survey on blockchain, SDN and NFV for the smart-home security,” Internet of Things, vol. 20, p. 100588, Nov. 2022, doi: 10.1016/j.iot.2022.100588.

[7] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, "A Survey on Role of Blockchain for IoT: Applications and Technical Aspects," Computer Networks, vol. 227, p. 109726, May 2023, doi: 10.1016/j.comnet.2023.109726.
[8] S. Nguyen, P. S.-L. Chen, and Y. Du, "Blockchain adoption in container shipping: An empirical study on barriers, approaches, and recommendations," Marine Policy, vol. 155, p. 105724, Sep. 2023, doi: 10.1016/j.marpol.2023.105724.
[9] T. Huynh-The et al., "Blockchain for the metaverse: A Review," Future Generation Computer Systems, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/j.future.2023.02.008.
[10] A. Kumar et al., "Blockchain for unmanned underwater drones: Research issues, challenges, trends and future directions," Journal of Network and Computer Applications, vol. 215, p. 103649, Jun. 2023, doi: 10.1016/j.jnca.2023.103649.
[11] X. Wang, H. Xie, S. Ji, L. Liu, and D. Huang, "Blockchain-based fake news traceability and verification mechanism," Heliyon, vol. 9, no. 7, p. e17084, Jul. 2023, doi: 10.1016/j.heliyon.2023.e17084.
[12] L. Turchet and C. N. Ngo, "Blockchain-based Internet of Musical Things," Blockchain: Research and Applications, vol. 3, no. 3, p. 100083, Sep. 2022, doi: 10.1016/j.bcra.2022.100083.
[13] Y. Wang, Q. Sun, and R. Bie, "Blockchain-Based Secure Sharing Mechanism of Online Education Data," Procedia Computer Science, vol. 202, pp. 283–288, Jan. 2022, doi: 10.1016/j.procs.2022.04.037.
[14] C. E. J. Singh and C. A. Sunitha, "Chaotic and Paillier secure image data sharing based on blockchain and cloud security," Expert Systems with Applications, vol. 198, p. 116874, Jul. 2022, doi: 10.1016/j.eswa.2022.116874.
[15] T. Zhang, B. Li, Y. Zhu, T. Han, and Q. Wu, "Covert channels in blockchain and blockchain based covert communication: Overview, state-of-the-art, and future directions," Computer Communications, vol. 205, pp. 136–146, May 2023, doi: 10.1016/j.comcom.2023.04.001.
[16] S. Zhang and S. Luo, "Evolution analysis of corporate governance structure based on blockchain network security and complex adaptive system," Sustainable Energy Technologies and Assessments, vol. 53, p. 102715, Oct. 2022, doi: 10.1016/j.seta.2022.102715.
[17] P. Bothra, R. Karmakar, S. Bhattacharya, and S. De, "How can applications of blockchain and artificial intelligence improve performance of Internet of Things? – A survey," Computer Networks, vol. 224, p. 109634, Apr. 2023, doi: 10.1016/j.comnet.2023.109634.
[18] S. Bonnet and F. Teuteberg, "Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: A multiple case study analysis," Computers in Industry, vol. 144, p. 103789, Jan. 2023, doi: 10.1016/j.compind.2022.103789.
[19] V. Merlo, G. Pio, F. Giusto, and M. Bilancia, "On the exploitation of the blockchain technology in the healthcare sector: A systematic review," Expert Systems with Applications, vol. 213, p. 118897, Mar. 2023, doi: 10.1016/j.eswa.2022.118897.

Authors:

DhanarajuMurala Received B.Tech (IT) degree from JNT University Hyderabad, Telangana and received M.Tech (SE) from JNT University Hyderabad, Telangana. Currently, He is a research 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, a distinguished academic with a Ph.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 AI/ML Domain Lead at GITAM University, Visakhapatnam, 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.