Section A-Research paper
ISSN 2063-5346

AN EFFECTIVE CIPHER TEXT POLICY ENCRYPTION METHOD FOR COLLABORATIVE BLOCK CHAIN DECRYPTION

Dr.Usha.M[1], Swetha.R[2], Dr.Pritto paul.P [3] , [4]Aminta Sabatini

Abstract

Block chain is a technological advancement that was developed using a variety of techniques, including math, physics, cryptography, financial models, etc. Block chain is a decentralized, digital ledger of all cryptographic currency exchanges. In this application, the land registration process on the block chain is used. This exchange includes administrative, buyer, seller, and registration office components. They essentially communicate in light of the local land registration process. The admin, seller, buyer, and register office must all register and login on the web page. In order to receive official approval and ship the buyer's purchase, the seller must provide the sub-register office with information about the land including the landowner, size, file, document, price, and other details. To make it easier for customers to monitor exchanges without maintaining a central record of them, all digital currency exchanges are stored in sequential order. The block chain's application potential is encouraging and has been showing results ever since it started. Although numerous studies on the security and protection issues of the block chain have been conducted, a thorough evaluation of the security of block chain frameworks is still lacking.

Keywords: *Cryptography, Block Chain, Encryption and Decryption*

[1, 3]Associate professor, Computer Science Department, Velammal Engineering College, India

[2] PG scholar, Computer Science Department, Velammal Engineering College, India

[4]Assistant professor, Computer Science Department, Velammal Engineering College, India

Corresponding Author: Dr.Usha.M**,** usha.m@velammal.edu.in

1. **Introduction**

In land registration using block chain, encryption and decryption are crucial for protecting the confidentiality and integrity of the data stored on the network. Two common encryption algorithms used in this context are SHA256 and AES. SHA256 is a hash function that is used to create a digital signature of a transaction, ensuring the integrity of the data and providing proof of authenticity. In land registration, SHA256 can be used to create a hash of the land title document, which can then be stored on the block chain. This hash can be used to verify the authenticity and integrity of the document, and to ensure that it has not been tampered with. DES, on the other hand, is a symmetric key encryption algorithm that can be used to secure sensitive data such as private keys or user data stored on the network. In land registration, DES can be used to encrypt the land

title document, ensuring that it can only be accessed by authorized parties who have the correct decryption key. Overall, the use of encryption and decryption techniques such as SHA256 and AES is critical for securing the land registration process in block chain. By ensuring the confidentiality and integrity of the data on the network, these techniques help to establish trust between the parties involved and promote transparency in the land registration process. Cipher text encryption is the process of transforming a message or data into an encoded or scrambled format to prevent unauthorized access or eavesdropping during transmission or storage. The encrypted message or data is referred to as cipher text, and the original unencrypted message or data is referred to as plaintext. There are many different encryption algorithms and techniques that can be used to encrypt data, including symmetric key encryption, asymmetric key encryption, and hashing. Symmetric key encryption involves using the same secret key to encrypt and decrypt the data. This method is typically faster than asymmetric encryption, but requires secure key exchange between the sender and the recipient. Asymmetric key encryption, also known as public key encryption, uses two keys - a public key. The frame work for SHA-256 is briefly explained below:

The commonly used cryptographic hash function SHA256 creates a distinct digital fingerprint from a message or piece of data. By using this digital fingerprint, the data's authenticity, integrity, and lack of tampering are all guaranteed. The following elements make up the SHA256 technology's framework,

Data types that can be included in an input message include text, files, and binary data. It is employed to keep a hashed copy of user credentials to prevent password cracking attempts.

The SHA256 technology foundation, in its entirety, is crucial for assuring the security and integrity of data across a range of applications and sectors.

- *Input message*: Data types that can be included in an input message include text, files, and binary data.
- *Pre-processing*: In order for the input message to be processed by the SHA256 algorithm, it must first be pre-processed to verify that it is a constant length. The message is pre-processed by adding a length parameter and padding it with zeroes.
- *Message compression*: To create a hash value, a pre-processed message is split up into 512-bit blocks and subjected to a number of mathematical processes, including bitwise operations, modular arithmetic, and logical operations.
- *Output:* The hash value is a 256-bit fixed-size output that acts as the message's own digital fingerprint. This output can be utilized for a variety of things, like confirming the legitimacy and integrity.

2. Overview of AES and SHA-256 Algorithm:

Administrator of this application endorses the registration office, which will then complete the land transaction and determine the cost. The land dealers make the land available to a specific buyer who will buy it, have it registered with the government, and build a patta or a citta. The structure uses SHA computations to hash the data and encodes it in blocks of 64 pieces each; hence 64 bits of plain text must be contributed by DES calculations. The 64-bit record that has been hashed and modified has been stored in a data set using block chain-based technologies like distributed availability and cross-networks.AES and the SHA algorithm are the two techniques.

Advantages: It is known to be error-free and has not been "broken," which is unusual for certain other well-known hashing techniques. It has no known flaws that would make it suspect, and it has not "broken," which is unusual for certain other well-known hashing methods. In order to provide an extremely high level of security, block chain technology is designed so that no block or exchange that joins the chain can be

changed. This technology is then used to store data in a decentralized manner so that everyone can verify the accuracy of the data by using zero-information verification, in which one party verifies the accuracy of information to another party without disclosing anything.

Scope includes,

Verbal understanding: The sale or purchase of the land may be agreed to verbally by the seller and the buyer. This can entail prioritising actual site evaluation and business interactions over estimating.

Agreement preparation: Once an agreement has been reached orally, it should also be documented in writing. The deal archive is then set up to complete this. Anyone can prepare the record, but it is advised that you seek legal counsel's assistance to ensure its veracity.Hence, there search information base utilized by the register office is mysterious. Regularly crisscrossing the name of Patta or Citta structure during land registeration process. In reality changing of name in patta structure ought to make an issue purchaser and dealer land and In the event that the entire degree of the place where there is a specific overview number has a place completely with an individual, the patta ought to remain in A s name as it were. Assuming some other different names are placed in that patta, you need to protest it and document an application to the Tahsildar/Zonal representative tahsildar of your area mentioning him to erase the name of the detached individual from that patta. In the event that the one section of land has a place with A&,B, the patta will be in the names of An and B mutually and will be called as joint patta.

The proposed protocol's operation are accomplised by the following modules ,

- Data Verification.
- AES Algorithm Implementation.
- Implementing Block chain with (algorithm-SHA 256)
- Hash key generator

Data Verification:

The data verification module is a crucial component of the land registration project, responsible for ensuring the accuracy and integrity of the information entered into the system. It plays a vital role in reducing errors, preventing fraudulent activities, and maintaining reliable land ownership records. The module incorporates various mechanisms and algorithms to verify the authenticity and consistency of the data.

AES Algorithm Implementation:

AES operates on blocks of data and supports key sizes of 128, 192, and 256 bits.AES uses a substitution-permutation network (SPN) structure with multiple rounds of transformations, including substitution, permutation, and key mixing operations. The algorithm operates on a 128-bit block of plaintext and applies a series of transformations based on a secret key.

Implementing Block chain with(algorithm-SHA 256):

The same input will always produce the same output hash value. SHA-256 can efficiently calculate the hash value for inputs of any size.

Hash key generator:

The output generated can include various documents and data related to land ownership and transactions with hash key generated file.

3.Description of block chain and algorithms

Block chain-Data is recorded and stored using block chain, a decentralized and distributed ledger technology, in a secure and open manner. In order to make the trade of crypto currencies like Bit coin easier, the technology was originally established in 2008. Its promise, though, extends beyond simple financial transactions. A block chain is fundamentally a database made up of a series of information-containing blocks. Using cryptographic

methods, each block in the chain is connected to the one before it, producing a safe and impenetrable record of all transactions or events. This creates a high level of trust and transparency since it makes it difficult for one person to change or modify the data contained on the block chain.

The decentralized aspect of block chain, which implies that there is no central authority or middleman regulating the system, is one of its fundamental characteristics. Instead, a network of computers, or nodes, validates and records transactions, making it more resistant to censorship and hacker attempts. Beyond crypto currencies, block chain technology offers a wide range of possible uses, including supply chain management, voting processes, digital identity verification, and more. It has the power revolutionize sectors by boosting productivity, cutting expenses, and enhancing security and transparency.

CP-ABE-Cipher text-Policy Attribute-Based Encryption (CP-ABE) is an advanced encryption technique that allows data to be encrypted and shared securely with multiple parties based on their attributes or characteristics. In CP-ABE, the attributes are associated with the user's secret key and the cipher text is associated with an access policy that defines the attributes needed to decrypt the data. This means that only authorized users with the appropriate attributes can access the encrypted data.

CP-ABE is used in various applications, including cloud computing, wireless sensor networks, and Internet of Things (IOT) devices, to ensure secure data sharing and access control. The use of CP-ABE can enhance the security and privacy of data sharing among multiple parties and provides a more fine-grained access control mechanism.

AES- IBM created the symmetric key block cipher algorithm known as the Data Encryption Standard (DES) in the 1970s. The National Institute of Standards and Technology (NIST) later approved it as a standard in 1977. A popular encryption method still in use today in a few applications is DES.

Data is encrypted in 64-bit blocks using a 56-bit secret key in the DES technique. A number of operations, such as permutations, substitutions, and transpositions, are used in the method. Festal rounds, a procedure that repeats these operations 16 times, results in a challenging and safe encryption method.

For many years, DES was thought to be a reliable encryption technique, but improvements in computing power have rendered it more susceptible to brute-force attacks. The Advanced Encryption Standard (AES) was created as a solution to this problem and has since taken the place of DES as the encryption algorithm of choice for most applications. Despite its flaws, DES is still used in some legacy systems and is occasionally combined with other encryption techniques to increase security.

SHA-256-Secure hashing is represented by the SHA algorithm. SHA is a modified version of MD5 that is used to hash data and legal documents. By using bitwise operations, isolated increases, and pressure capabilities, a hashing calculation condenses the data into a less lavish structure that is imperceptible. Can hashing be broken or unscrambled, you may wonder? The primary difference between hashing and encryption is that hashing is one-way; once the information is hashed, the resulting hash digest cannot be broken, unless a vicious power attack is used. The SHA calculating process is shown in the image below. SHA operates in such a way that it will generate a different hash even if only one person changes the message.

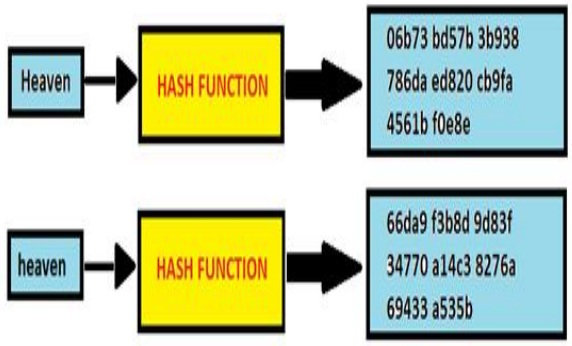

Figure 2.4 Flow of hashing

The underlying message is the hashing with SHA-1, bringing about the hash digest will be codehash"06b73bd57b3b938786daed820cb9fa4 561bf0e8e".In the event that the second, comparative, message is hashed with SHA-1, "66da9f3b8d9d83f34770a14c38276a69433a535 b".This is alluded to as the torrential slide impact. The fig 2.4 illustrates the impact is significant in cryptography, as it implies even the smallest change in the information message totally changes the result. This will prevent assailants from having the option to comprehend everything that the hash digest initially said and saying to the beneficiary of the message whether the message has been changed while on the way. As recently referenced, Secure Hashing Calculations are expected in all advanced marks and declarations connecting with SSL/TLS associations, yet there are more purposes to SHAs also. Applications for example, SSH, S-Emulate (Secure/Multipurpose Web Mail Expansions), and IPSec use SHAs too. SHAs are additionally used to hash passwords so the server just has to recall hashes as opposed to passwords. Along these lines, in the event that an aggressor takes the data set containing every one of the hashes, they wouldn't have direct admittance to all of the plaintext passwords, they would likewise have to figure out how to break the hashes to have the option to utilize the passwords. SHAs can likewise fill in as signs of a record's trustworthiness. In the event that a document has been changed on the way, the subsequent hash digest made from the hash capability won't match the hash digest initially made and sent by the record's proprietor. Thus now realizing what SHAs are utilized for, yet why utilize a Solid Hashing Calculation in any case, A typical explanation is their capacity to stop aggressors. However a few strategies, similar to savage power assaults, can uncover the plaintext of the hash processes, these strategies are made incredibly troublesome by SHAs. A secret phrase hashed by a SHA-2 can require years, even a very long time to break, in this manner squandering assets and energy on a straightforward secret key, which might dismiss numerous aggressors. One more motivation to utilize SHAs is the uniqueness of all the hash digests. If SHA-2 is utilized, there will probably be not many to no crashes, meaning a straightforward difference in single word if a message would totally change the hash digest. Since there are not many or no impacts, an example can't be found to make breaking the Protected Hashing Calculation more straightforward for the assailant. These are only a couple of justifications for why SHA is utilized so frequently.

4.Stratergies of implementation

There are a number of tactics you may use when implementing a safe hash algorithm to guarantee the reliability and security of the hashing operation. Here are some crucial tactics to take into account:

1. Select a Strong Hash Algorithm: Pick a hash algorithm that is well-known and cryptographically safe, such as Blake2, SHA-256, or SHA-3. These algorithms have undergone thorough examination and are thought to be secure.

2. Salt the Input: Before hashing, add a distinct salt value to the input data. Particularly in situations where the same input data is likely to be hashed numerous times, salting introduces randomization and blocks precompiled attacks.

3. Iterative Hashing (Key Stretching): Use a method like key stretching to repeatedly run the

hash algorithm. By lengthening the computing process, the hash becomes more robust against brute-force and dictionary assaults.

4. Implement Length Extension Protection: Ensure that the proper steps are taken to mitigate this vulnerability if the hash method is prone to length extension attacks . Use more recent hash algorithms that naturally defend against length extension attacks.

5. Validate and sanities: the input data to ensure that no malicious or unexpected data types can interfere with the hashing operation. Edge situations, managing various character encodings, and verifying that the input follows expected formats are all included in this.

6. Security Testing: To find and fix any implementation flaws or vulnerabilities, do thorough security testing, including penetration testing and vulnerability assessments.

7. Peer review and code auditing: Ask seasoned programmers or security professionals to assess your implementation so they can look for potential bugs or vulnerabilities in the code.

5. Outcome

A secure hash algorithm produces a fixed-length character string known as the hash value or digests as its output. A secure hash algorithm's essential characteristics include:

1. Deterministic: The method always returns the same hash value for a given input. Data that has been hashed can be checked and compared thanks to this attribute.

2. Irreversible: Recovering the original input data from the hash value is computationally impractical. The hashed data cannot be quickly reversed or decrypted because to this characteristic.

3. Unique: Various inputs should result in various hash values. There should be a noticeable difference in the hash value even with a minor change in the input. Hash values can now serve as distinctive identifiers for data integrity tests thanks to this attribute.

4. Uniform Distribution: A secure hash algorithm should distribute hash values uniformly across the entire output space. This property helps avoid collisions, where two different inputs produce the same hash value.

5. Fixed Length: The hash value has a fixed length, regardless of the input data size. This allows for efficient storage and comparison of hash values.

6. Sensitivity to Input Changes: Even a small change in the input data should produce a completely different hash value. This property ensures that even a minor alteration in the input will result in a significantly different hash value.

The outcome of applying a secure hash algorithm is primarily used for data integrity verification, password hashing, digital signatures, and various cryptographic protocols. It provides a compact representation of the input data, making it useful for comparing large amounts of data efficiently and securely.

6. Methodology

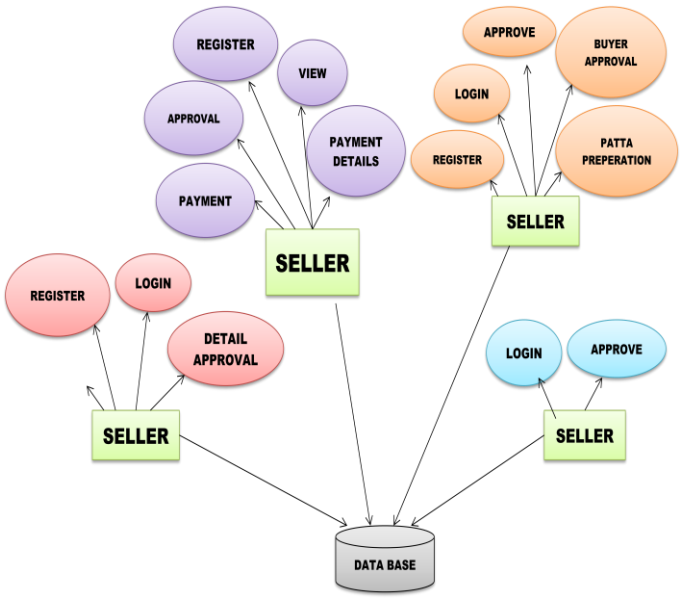

Figure 6.1 Methodology of study

The systems architect establishes the basic structure of the system, the proposal of Hash code Solomon algorithm and accessing a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of this scheme has been validated, which is really a powerful supplement to existing cloud storage.

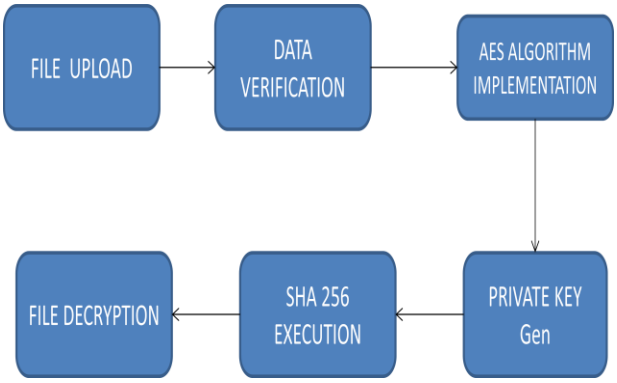

Figure 6.1.Architectural flow

The structure of flow from uploading the file by verification of all credentials it moves to the next phase of implementing AES(Advanced Encryption Standard)with this encryption a privatekey value is generated and the generated key value is then used for decrypting the file.

Hash value is generted using SHA-256 this executes the specific value that is used to decrypt the file. Fig(6.1)Architectural flow explains the structure of file flow from the stage one to decryption phase,AES algorithm plays the major role in implementing the encrypted values using SHA-256 algorithm with message digest.In the event that a document has been changed on the way, the subsequent hash digest made from the hash capability won't match the hash digest initially made and sent by the record's proprietor. Fig (6.2) explains the Processing of operation flow is represented below with the relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure. For each data flow, at least one of the endpoints (source and / or destination) must exist in a process. The refined representation of a process can be done in another data-flow diagram, which subdivides this process into sub-processes.

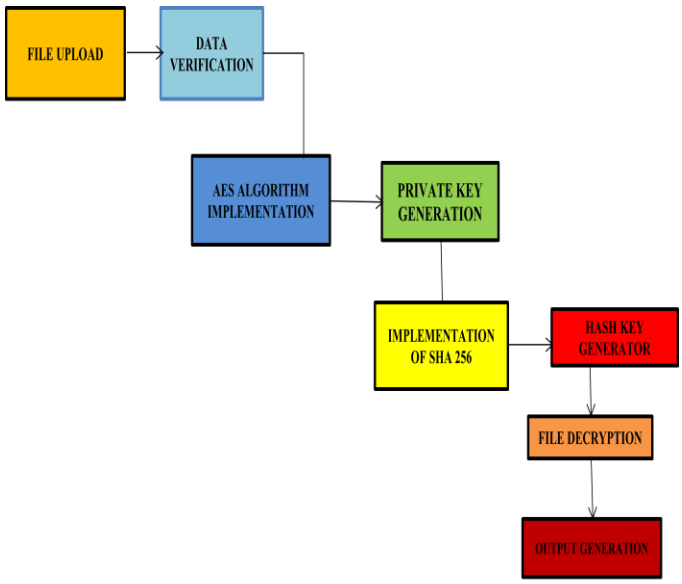

Figure 6.2 flow of the process

7. RESULTS AND DISCUSSION:

In future execution will add a calculation to carry out the task exceptionally secure. Furthermore, add some module or states to work on additional choices to execution.

The graph represents the collaborative attributes of the data generated in the framework.

Future advantages are,

- Safe and Secure.
- Analyze the file list then control

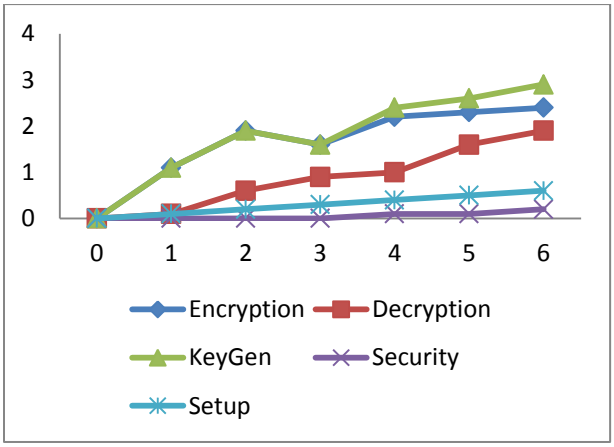

Figure 7.1 Analysis of data framework

This graph represents the connections and relationships between different entities in a network. It can be used to visualize network infrastructure, identify potential vulnerabilities, and track network traffic flows with less security.

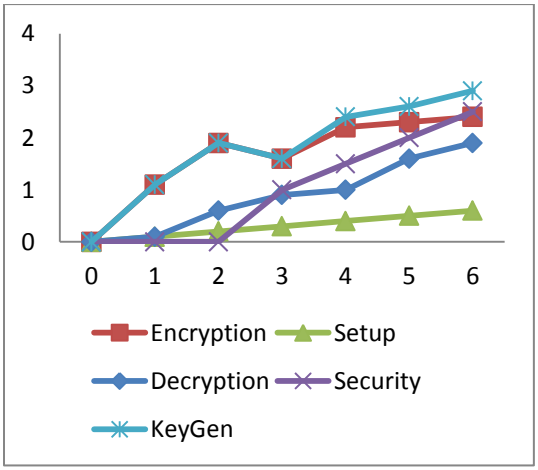

Figure 7.2 attributes of proposed framework

This graph represents the flow of security with both encryption and decryption with the accuracy of safe flow of data.

8. CONCLUSION:

This association incorporates executive, buyer, seller and registration office. On a very basic level they convey themselves thinking about nearby land registration process. In site page key choice and login worth of overseer, seller, buyer and register office. Merchant give land subtleties like landowner, size, record, report, cost and different subtleties to sub-register office for getting endorse from official and shipped off purchaser. The exchanges of cutting edge financial principles are all dealt with in progressive sales to help clients in following the exchanges without remaining mindful of any focal record of the exchanges. Application possibilities of block chain are promising and have been conveying the outcome since its introduction. However various assessments have been done on the security and protection issues of the block chain a deliberate assessment on the security of block chain frameworks is right now absent. So these have put out a seamless, user-friendly, and seamless platform that might be applied to speed up land registration. There are numerous problems, including schedule delays, vendor engagement, or intermediate involvement. The problems with land registration in India and many other countries will be resolved as a result of this forum. The article includes a detailed description of the procedures which make up the land registration process. The process will be made simpler by deregistering land titles, which will also protect them from countless man-made and natural disasters. Block chain technology is advancing swiftly due to its consistent capabilities. So, one way to create static records is to use a block chain to store world record transactions. Therefore, the main challenge for this solution will be to generate safe and secure framework to the proposed one.

REFERENCES

Zhaoqian Zhang, “An Expressive Fully Policy-Hidden Ciphertext Policy Attribute-Based Encryption Scheme With Credible Verification Based on Blockchain,”in *IEEE Internet of Thingsl*, Volums, Issue: 11, 01 June 2022.

Ruizhong D, “Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Block chains” in *Tsinghua Science and Technology*, Volume: 28, Issue: 1, Feb 2023.

.
Banerjee et al, "Multi-authority CP-ABE-based user access control scheme with constant-size key and cipher text for IoT deployment," in *IEEE INTERNET OF THINGS JOURNAL*, J. Inf. Security Appl., vol. 53,Aug. 2020.

M. Xie, J. Hu and H. Hong, "Blockchain-based CP-ABE with publicly verifiable outsourced decryption in IoT," in *IEEE INTERNET OF THINGS JOURNAL*, pp. 3-18, 2020

Ying He,"An Efficient Cipher text-Policy Attribute-Based Encryption Scheme Supporting Collaborative Decryption With Block chain," in IEEE INTERNET OF THINGS JOURNAL, VOL. 9, NO. 4, FEB 15, 2022

Jasvant Mandloi, Pratosh Bansal, "An Empirical Review on Blockchain Smart Contracts: Application and Challenges in Implementation", International Journal of Computer Networks and Applications (IJCNA), 7(2), PP: 43 - 61, 2020

Pravin Soni, Rahul Malik, "Efficient Cipher Scheme for Hybrid Models with Internal Structure Modification", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 596-606, 2021

Abdualrahman Johari, Raed Alsaqour, "Blockchain-Based Model for Smart Home Network Security", International Journal of Computer Networks and Applications (IJCNA), 9(4), PP: 497-509, 2022.

R. Langrehr and J. Pan, "Tightly secure hierarchical identity-based encryption", J. Cryptol., vol. 33, no. 4, pp. 1787-1821, 2020.

Adnan Nadeem, "A Survey on Blockchain Technology: Evolution, Architecture and Security"in ,IEEE Access, Volume: 9, 2021.

Shafarenko, A. A PLS blockchain for IoT applications: protocols and architecture.in springeropen **4**, 4 (2021)

Malomo, O., Rawat, D. & Garuba, M. Security through block vault in a blockchain enabled federated cloud framework. In springeropen *Appl Netw Sci* **5**, 16 (2020).

Yan, L., Ge, L., Wang, Z. *et al*. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment"in springeropen*J Cloud Comp* **12**, 61 (2023)

M. R. Alves, P.G., Aranha, D.F. "A framework for searching encrypted databases."in springeropen *J Internet Serv Appl* **9**, 1 (2018)

Liu, H., Tai, W., Wang, Y. *et al.* "A blockchain-based spatial data trading framework".in springeropen *J Wireless Com Network* **2022**, 71 (2022).

.

Section A-Research paper
ISSN 2063-5346