ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

Timestamp Hashtag for BC-LPBFE: Block Chain Security Using Lattice Verified Pair-Block Folding Encryption For Improving Integrity Proofing In Cloud Environment

K. GANGADEVI[*1] , R.RENUGA DEVI[2]

[*1] Ph. D Scholar, VELS University, Pallavaram, Chennai, India

[2] Assistant Professor, VELS University, Pallavaram, Chennai, India

Abstract

Blockchain is one of the developing security strategies to allow the transaction based on cryptographic approaches. Due to security breaches in data sharing and privacy vulnerabilities that cannot be ignored for a long time due to attackers. To address these shortcomings, this paper proposes a blockchain-based method of sharing data with decent security. We propose a Timestamp Hashtag-based blockchain security using Lattice Verified Pair-block Folding Encryption (BC-LPBFE) for improving integrity proofing in the cloud environment. Initially, access credential-based security was created based on integrating Lattice-based Access Control Generation (LBACG). This creates user and owner policy roles to access the data on each authentication and verification. Lattice point creates Access Control Role Matrix (ACRM) to provide permission. Then the blockchain process creates a Timestamp HashTag Key (TSHT) for each block random session key with the same length of the key with equalized block size. Further, the key is embedded with each block to make Pair-Block Folding Encryption (PBFE), during this encryption the blocked data are streamed into Lattice Bit Plane Transformation (LBPT) at running encoded data length to decrease the storage size and performed into folded blocks. Finally the Roll Back Key Verification (RBKV) the key is singularized to encrypted, during decryption keys are verified at each block to retrieve the original data. This proposed system produces the best performance compared to the other system as well in security improvement.

Keywords: blockchain security, Hash function, Pair-Block Folding Encryption, cryptography, key verification, timestamp security.

1. Introduction

Cloud computing offers various levels of data management processing, storage from a decentralized environment. This provides user-friendly services based on the end-user requirement. Cloud environments maintain different data resources for different organizations. Due to the nature of centralized data processing and storage, security is an important concern to protect user data from outside of unauthorized user access. Depending on the user requirement services to be provided through software system storage, network, and virtualized environment service access to the user. The cloud service provider offers various data to access cloud resources. So all the service providers improve the security maintenance in different concerns based on role-based accessed secured concerns

Blockchain security plays an important role in the field of information security in a transactional environment. Widely used to provide data integrity, message authentication, digital signatures, and password protection. Therefore, we have proposed Blockchain technology so that you can pay a fee to provide access to patient medical reports. It uses Blockchain technology 3 levels 1. Authentication, 2. Encryption and 3. Data recovery.

This framework proposed may ensure patient safety and maintain the safety and reliability of private data sharing systems. Analysis of existing programs reveals that cryptographic failures and sharing of a program based on Blockchain cannot successfully implement data-intensive access control of existing personal health records. These centralized management systems are at risk of privacy leaks. It requires the integration that the user wants to check the cloud. Aiming at these issues under the existing plan, in this paper, we will examine that we propose a new personal health record that completes the plan based on the data and shares Blockchain.

All the users still have access service differently and specifically, the services offer a storage medium based on the log of account to store the data. This depends on sharing the registering assets among the servers and the applications, additionally, it has risen as another worldview for facilitating and conveying the security services over the Internet is role-based access control. Users must be controlled to accessing data with various restrictions. It can find any information about multiple users who have to protect the cloud from access to wrong access. To solve this, here novel security based on crypto policy approaches are used to increases the security in services against attacks

Storing sensitive data is an essential need for each user to keep the personal data safely without access from another user in the cloud. So security and privacy is an important factor consideration to protecting the sensitive data. In this way, the personal health records contain sensitive data about the patient's information which keeps private information in the

public cloud. By this data, maintenance is important to keep security and access rights to protect sensitive information.

The role-based access is primary security to access the data by providing administration permission to read, write or modify, delete, or both combinational access permission to set the role to the user account. Based on the access permission the user access the data on the cloud account. Similarly, data protection is carried to protect the data through cryptography techniques which are works upon the principle of encryption and decryption.

The user access is based on a log of authentication mode from a cloud account to keep the data in encrypted mode with a security key. Initialization security depends on the Encryption using plain text converted into ciphertext using a different encryption algorithm.

All over the data stored in the cloud is based on upload and download depending on the user and administration request and response. The storage concerns are formalized in encryption type to secure the content. This is work on the principle of converting the original text or attributes into ciphertext formatting with a characteristic format based on the symmetric and asymmetric level security. The encryption and decryption are based on the key on authentication weather permitting the user the right keys to access the data. The existing approach depends on various ways and formats with key levels to make encryption, for example, RSA, DES, AES-based encryption, and decryption are balanced based on the authentication and auditing key-based security to protect the data.

The contribution research is designing efficient access role-based security crypto policy algorithms to support the performance development of cloud privacy based on blockchain security. The cryptographic algorithm should be capable of restricting malicious access from genuine and illegal users. The malformed access request would even come from genuine registered users. Still, the algorithm should identify such malformed access and restrict them.

The service request would contain much information and the user access details are available with the system. Using this information, the algorithm should compute dissimilar procedures in limiting illegal access. The algorithm should be capable of restricting malicious access from genuine and illegal users. The malformed access request would even come from genuine registered users. Still, the algorithm should identify such malformed access and restrict them. The service request would contain much information and the user access details are available with the system.

Using this information, the algorithm should compute dissimilar procedures in limiting illegal access. The primary purpose of the work is to improve the privacy-preserving during data in personal health records.

2. Related work

Blockchain is digital chaining data security that has gained significant importance. The service is provided by the CC based on the request and the amount is paid to the service provider, but this is a "service" that arbitrarily creates and establishes an art service, focusing on its use. Offering a privilege, [1, and 2]. Cloud resource pricing is also based on usage [3]. Patients are classified as having and providing, as well as health systems, computing auction services, easily [4] sharing their health details with other organizations in the cloud.

That cloud storage negatively leads to a model as a security service that exits it [3]. Generally, storage security is completely controlled by the service provider and there is always the possibility of data failures [4]. At the other end when security is compromised, ensuring the confidentiality and integrity of user data in the cloud becomes a challenge.

Encryption is primarily a function used to provide users with data protection and privacy of their information [5]. It helps the user to convert the original information into cryptographic information using the private key. Today's Views Encryption is the only way to store data on shared resources in cloud computing that provide complete privacy [6]. Therefore, various types of standard encryption have been introduced to improve the security of shared resource data as well. Such encryption standards include stock-based access, identity-based access, and attribute-based access [7].

Privacy concerns for limiting One natural way is to allow data owners (DOS) providers to additionally load PHRs encryption into the cloud. However, in such a cloudy open network, confidential information may be stolen using these unauthorized persons [8]. It is important to create a well-protected framework for sharing data that address these issues that exist in health domains.

Nonetheless, in the health-care domain, '3' factors are significant: privacy, security, besides, interoperability [9]. However, the researchers have utilized key-policy attributes-based encryptions (KP-ABE) aimed at safe Access Control (AC). In KP-ABE, the attribute authority issues the users' key [10]. It signifies which sort of Cipher Texts (CT), the key can decrypt, whilst CT is tagged utilizing the sender with a compilation of descriptive attributes [11].

Cloud providers aim to provide the best services, although each service provider will give some practical ambiguity lies based on usage. Cloud users sometimes store large amounts of their data, which they may suffer from vulnerabilities and impacts [12]. Since the controls are only partially above the stored data, users need strong and significant security techniques to protect their data. Protecting User Data from Protecting Data Protection Protecting data storage is a challenging and intimidating task. So that better control of the direction to achieve precise AC [13] can now be accessed. The secrecy of classified and based encryption (Communist Abe) data is an excellent location.

In CP-ABE, any user is represented using a compilation of attributes. Additionally, CT is created beneath a provided access policy [14]. One secret key will be utilized to decipher a particular CT, provided that, the attributes associated with this SK meet the policy written in CT [15].

A Blockchain-Based routing algorithm for IoT is discussed where the BCR approach uses the contracts in discovering the route which is secure for data transmission [16]. A fuzzy rule-based trusted secure routing algorithm is presented in [17], which measures the trust value according to the fuzzy rule available

This work primarily focuses on designing secure methods to provide the reliability and privacy of patient information. Cancer patients face this challenge because data access control requires security, reliability, and access reliable

data transfer based on proposed BC-LPBFE implementation proves the best performance.

3. Timestamp Hashtag based blockchain security using Lattice Verified Pair-block Folding Encryption (BC-LPBFE)

In this proposed implementation Hash policy blockchain-based cryptography technique is intended to improve security. Timestamp Hashtag-based blockchain security using Lattice Verified Pair-block Folding Encryption (BC-LPBFE) for improving integrity proofing in the cloud environment. The hash access policy created the role of user authentication policy Depending on lattice access control. Initially, the security begins with authentication levels based on the registration, user credentials, the role of the account, and administration providence. The user credentials are authentication by admin rights by each logon the behavior of the user is monitored by the cloud access controller. User access levels are monitored and stored the values as features, the features are considered as the monitoring logs to make an analysis. Using the attribute analysis as a feature case using the Principle component analyses model to select the feature weights. Based on the weightage the user be authenticated to access the account.

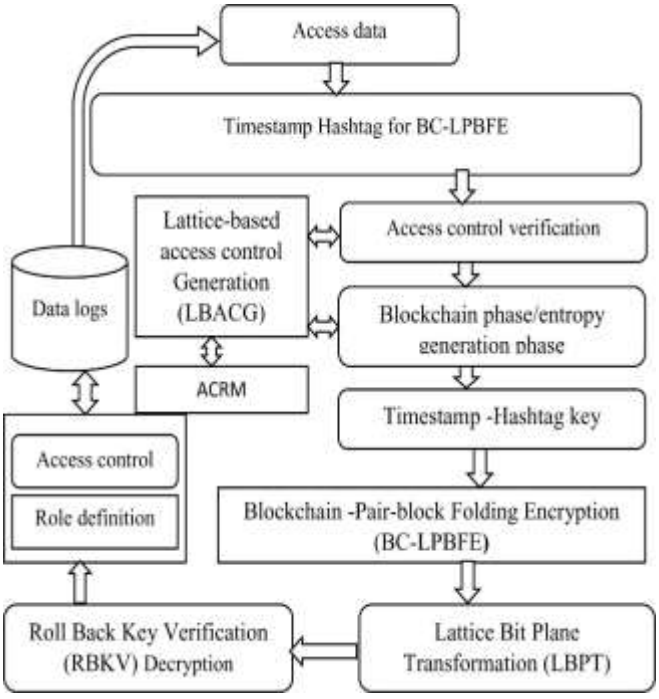

Figure 1 Lattice Verified Pair-block Folding Encryption (BC-LPBFE)

The proposed method of Pair-block Folding Encryption is enhanced with a lattice-based bit plane transformation technique (LBPT) shown in figure 1, which selects the role-based security using create Access Control Role Matrix (ACRM) scheme for improving security and reliability. Here the polynomial-time series approach improves in the ciphertext creation process.

The security of the proposed method is higher because the data is encrypted based on the lattice vector mapping instead of bilinear mapping. The polynomial setup makes it for the hacker too difficult to break the ciphertext. The lower the polynomial value greater the secured cipher. Because the ciphertext generated will be the complex one due to the hashing and lattice mapping process.

In this, the ciphertext policy setup is initiated by initializing the pairing group schemes, and methodology. The attributes are selected based on the polynomial vectors as input. The information of the user is collected through the login phase. The login phase is verified with stored credentials to store the data. If the credential is matched, the further process will take place otherwise the failure message is displayed. The public key will be generated for the patient based on credentials. The data will be encrypted with the public key. The ciphertext data will be stored in the cloud. Based on the access rights of the doctor or patient, the secret key pair for the user is generated to access the data. If the secret key pair is matched, then the data will be decrypted.

3.1 Generate Lattice-based access control Generation (LBACG)

In this phase, the initially verified authenticity provides a category-based role of access verification using a role-based access control called Lattice. The access control security begins to categorize policy-based roles to verify the user, accessibility role, owner policy, who are all to access the data. This method protects the private from unauthorized access initially as they verify the access from Logon policy.

Input: Private transactional Records
Output: Access control lattice
Step 1 : Process: verify the initialized credentials
Step 2: Compute while each record value as i
Initiate respective level of the values
Build a relationship through and protocol policy to access the data
Do end
Step 3: allow Authentication on initialization account control
Step 4:Return access Log

The proposed Double standard Encryption (DSE) algorithm provides more security in data wiring organization. By the object consideration, the user roles are used to set the secret value from lattice L. that have a good relationship with each other. The access level lattice L is as given in (1)

$$\text{Lattice } Lc = \text{Role}C_i * Y\text{access} \quad \ldots..(1)$$

Wherever Ci is the created user policy and Y is traditional of supplementary constraints from initial objects consideration $1 \leq i \leq n$ represents the additional rights access $C_1 > C_2 > C_3 \ldots > C_n$is under the user role haven the secret values to produce security.

3.2 Access Control Role Matrix (ACRM)

To create an Access Control Role Matrix (ACRM), Security includes access to shared resources to protect unauthorized access. The difference between authentication and unauthorized access is verified by the role from the subjectivity representation in the matrix point. Figure 5 shows the Access control matrix. The access control matrix creates the

user and document correlation matrix is completed depending on the object access policy as shown below,

Subject role/users	Document 1	Document 2	Document 3	Document 4
User 1	Owner-read-write, delete access control	Owner-read-write, delete access	Owner-read-write, delete access	Read access control
User 2	Read access control	Owner-read-write, delete access	write access control	Read access control
User 3	Read-write access control	Read access control	Read access control	Owner-read-write, delete access

Figure 2 Lattice-based Access control matrix

To secure the data, the data storage is to be accessed through the access control matrix values. This must perform an authentication process and then update with new data items. After verification, the user gets authorization to process the records in a double security modified format.

3.3 Block chain phase

Splitting the document separates the entire document into smaller portions that are pertinent for processing. A collection of document sets encompasses a mass portion of data and hence keyword search becomes crucial. For this, the input data is partitioned as minute portions to simply extract the features existent in the input data. $\Delta D = \{D_1, D_2, D_3 \ldots D_t\}$ is concerned as the input. Every document in a dataset is assigned to indistinguishable parts $\{s_1, s_2, \ldots s_t\}$. Whereas, the first split D_1 is signified as

$$P_1 = D_1\{s_1, s_2, \ldots s_t\}$$

Where t specifies the number of words in a document. Splitting is separately done for every document $\{D_1, D_2, D_3 \ldots D_t\}$ in the set and is saved in a separate array $S_{[i]}$

$$S_{[i]} = s_1 + s_2 + s_3 + \ldots s_t$$

Where $s_t = Splitted\ \ array\ of\ \ t^{th}\ document\ \ (D_t)$.

Based on the access control the logical condition creates the Blockchain by pointing array of Prof of stack to control the data access based on the access policy.

3.4 Entropy Indexing hash tree

Entropy is an essential terminology in information theory to estimate the quantity of data that can well be compressed. The entropy H itself gauges the average uncertainty of a single arbitrary variable L :

$$H(p) = H(L) = \sum_{x=X} p(L)\log_2 p(L)$$

Where $p(L)$ implies the probability mass function of the arbitrary variable L and the above equation tells us the average bits that are needed to represent all the information L. For example, if the requested document to be retrieved make L be the chance of attaining the required results. L will be a binary random variable. These entropy values acquired are utilized in the index tree generation.

3.5 Timestamp -Hashtag key generation

In this stage, the user generates the security for preventing data access based on blockchain crypto policy. The user selects the data and applies the block splitter by creating blocks with the sequence of continuous block Id. Each block contains a Block id hashcode with the time-stamped encrypted randomized key. This makes additional security during the block-based verification to decrypt the data. If any sequence is missing during the transaction verification, the entire process is rolled back for the safety process.

Algorithm: Timestamp -Hashtag key algorithm

Input: characteristic Numeric Key pattern
Output: Hash code key
Step 1:Start
Number and alphabetic formal [0-9, a-z], Formal = in
Step 2: compute each block Id
If (id==0)
{
Add Round Key (formal, w [0, Key-1])
For pattern key= 1 step 1
Split Number and alphabets (formal)
Formalized to shift the data rows
Shift to randomize mixing row and columns
Add pattern Key (check if any key
Compute formalized terms, W [forum pattern Securitykey* (Reqpattern Key +1)-1])
End for
Add pattern Key format (formalization, [w *NA, with doc(NA+1)*NA-1])
}
Else
{
returnOut = formalized data forum
}
Step 3: Return Formalized key
End

The above algorithm shows the hash code generation based on the time stamp intent to each block which is encrypted by advanced crypto policy standard. This provides a randomized pattern to add the additional key to the block to make improved security.

3.6 Lattice access control policy

A Data owner sets up the system using granting AC to Data User as well as uploading documents to the cloud. The Data owner possess a compilation of n documents such as,

$$D_s = \{z_1, z_2, z_3, \ldots\ldots\ldots, z_n\}$$

Where D_s denotes the data set and z_n indicates the n-number of data in the dataset

3.7 Pair-block Folding Encryption (BC-LPBFE)

The proposed method uses the data to be transferred between the source and destination. The method uses homomorphic encryption, where the input data is first split into matrix format and generates a public and private key to perform encryption. Finally, the cipher is changed to data and stored in the cloud. The cipher-generated data has been given to the user at the data access request and the user can decrypt the cipher data to get the original data.

Algorithm: Pair-block Folding Encryption (BC-LPBFE)
Pseudo Code
Input: Data Bpd
Output: Cipher Data CBpd
Start
Read input data.
BpdMat = Convert Data into matrix.
Public Key Pk = Generate Public Key
Private Key prk = Generate Private Key
For each index of matrix
Perform encryption with Prk and Pk.
End
Convert matrix into Cipher data CBpd.
Stop

The above discussed pseudo Code shows how data encryption is performed to enforce data security. The data has been converted into the matrix and using the private and public key, the encryption is performed. The encrypted matrix has been further converted into data.

3.8 Lattice Bit Plane Transformation (LBPT)running length encoder data

Running length encoder data RLE can be utilized on just one of the characters (as with the zero below), several, or all of the characters.

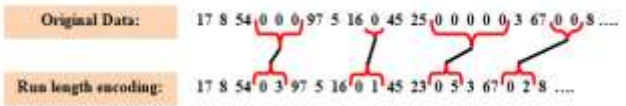

Figure 3 Examples for RLE

Example of RLE as exhibited in figure (3): every run of zeros is swapped using '2' characters on the file (compressed): a zero to specify that compression is happening, followed through the number of '0' on the run. The RLE format is given in the below equation,

$$C_f = P_c \| I_t \| R_c \otimes A_s$$

Where C_f denotes the compression format, P_c represents the special character indicating compression follows, I_t signifies any repeated data character, and R_c indicates the character count.

In this proposed methodology, the ASCII value A_s is computed for the particular character, which is multiplied with the count value R_c for reducing the traversing time.

3.9 Singularized Key generation data block

Initialize hash matrix: A 8×8 matrix of bytes is utilized to hold intermediary as well as last outcomes of the HF. The matrix is initialized as encompassing of all zero-bits.Process message in 512-bit block: The BC is the heart of this process, which is designed on the basis of the extensive trial strategy. Its block size and the key size are 512 bits, respectively. In its 10-round transformations, each round operates on a state of 8×8 bytes and updates the state via the sequence of the subsequent layers:

$$A_k \otimes M_r \otimes S_c \otimes S_b$$

Where S_b denotes the sub bytes, S_c represents the shift columns, M_c indicates the MixRows and A_k signifies the AddRoundKey. The sub Bytes is the non-linear transformation, layer, which implies the S-box to every byte of the state separately. The shift columns are the cyclical permutations layer that rotates the byte of column 'o' downwards through 0-1 positions. The MixRows is the linear diffusions layer that is a right-multiplication using a 8×8 row-oriented matrix, signified by R.

In AddRoundKey the key addition layer adds the round key to the state. In this whirlpool HA, the collision problem is occurred. So, this proposed methodology considers the double hashing for the avoidance of collision problem. The double hashing is expressed as follows,

$$\left(h_1(key) + I_t * h_2(key)\right)\%T_s$$

Where S_b denotes the subBytes, S_c represents the shift columns, M_c indicates the MixRows, and A_k signifies the AddRoundKey. Based on these generated has codes the hash tree is generated.

3.10 Timestamp Blockchain key verification

By applying the homomorphic exhibit of a disseminated check of expulsion coded information, our course of action satisfies the join of the point of confinement rightness

protection and information failure containment in cloud evaluating.

Algorithm: Time stamp Blockchain key verification
Information: Cloud information CD, Asset Table At
Yield: cloud altering effectiveness
Start
Get a CD for Req.
In case Req.Type==UpAttribute Auditing Then
Strengthen the advantage Table AT.
At = $\sum$ $[\![(CDi \in \backslash time) \cup Req.Resource]\!]$
Else if Req.Type==Entrance Then
Check with resource.
On the information chance that Unaffected at that point
Return attribute
End
End
Stop.

Open basic suitability task plot with single key storing per user. Our development depends on substance game plan trademark determination with ward keys. It decreases people in general storage necessity of existing plans, while additionally weakening the mystery storage cost at the focal expert. Public security and execution examination exhibit that the proposed arrangement is extraordinarily capable and adaptable against assuming discontent, destructive data alteration assault, and significantly server conspiring strikes.

3.11 Pair-block Folding Decryption

The encrypted data received from the server-side is used to perform decryption. The method uses Pair-block Folding Decryption, where the input data is first split into matrix format and decrypted with the public and private key to reverse-opening the data. Each matrix index feature has been decrypted with the key and decrypted matrix data has been used to generate the original data.

The proposed method reads the data and converts it into the matrix which is then decrypted with private keys. The decrypted matrix elements are reframed to produce the original data.

Algorithm: Pair-block Folding Decryption
Input: Cipher Data CBpd
Output: Original Data Bpd
Start
Read cipher input data.
Read public key Pk and private key Prk.
CBpdMat = Convert Data into matrix.
For each index of matrix
Perform Decryption with Prk.
End
Convert matrix into original data Bpd.
Stop

The above discussed pseudo Code shows how the data decryption is performed to enforce data security. The data has been converted into the matrix and using the private key, the decryption is performed.

4. Result and discussion

Blockchain security has been tested under the centralized cloud platform by acceding the data through access control mechanisms. Timestamp Hashtag-based blockchain security using Lattice Verified Pair-block Folding Encryption (BC-LPBFE) for improving integrity proofing in cloud environment. The results are tested to access the user–owner relation based on client–server request response model. The results are compared with sub-Enc, Ceaser cipher, SHA, Tri-DES, S2OPE, RSCRE. The security verification begins at the time of access tested with simulated user control on logon policy. The table given below shows the parameter taken to process the value in this environment.

Table 1: Environment variables and values processed

Platform and environment	**Values taken**
Cloud environment	AWS web service
Number of user	100
Development environment	Visual Studio C#.net framework
Data set	Collective document data
Cloud storage	EBS type 1

Table 1 shows the simulation parameters used in the proposed approach to test the security performance using the visual studio framework. This takes T3x large AWS server configuration to run remote mode to verify the security.

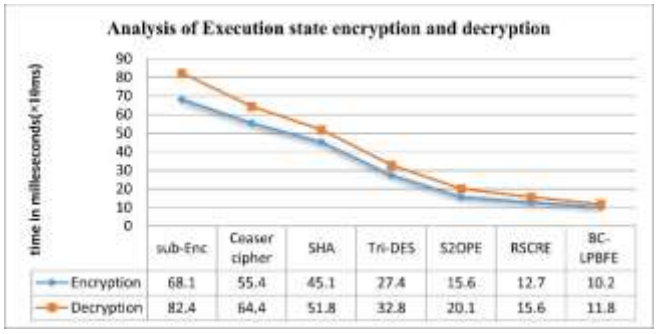

Figure 8: Comparison of execution efficiency

Figure 8, shows the efficiency of the execution state processed between encryption and decryption. The proposed system provides a substitution meantime as well as CPVPA cipher policy. This BC-LPBFE implementation has much-improved performance compared to previous methods.

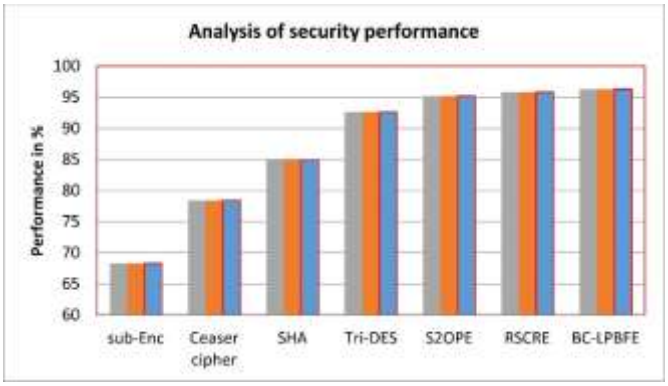

Figure 9: Comparison of security analysis efficiency

Figure 9 shows different methods of analysis produced by the different levels of user to analyze the security. The proposed system produces a higher impact on security performance compared to the other dissimilar methods.

Table 2: security performance

Methods	security performance in %
sub-Enc	68.3
Ceaser cipher	78.4
SHA	84.9
Tri-DES	92.6
S2OPE	95.2
RSCRE	96.1
BC-LPBFE	96.8

Figure 8and Table 2 show the comparison of the Security analysis, and this can be tested with the total number of users that access the security with the right authentication to access the data. The proposed system produces 95.2% accuracy compared to the other methods. The proposed system BC-LPBFEproves the great performance of higher-end security with the improvement of standard crypto advanced efficiency.

Time complexity (Ts)=$\frac{Total\ number\ of\ blocks\ per\ bits \times two\ phase\ encryption}{time\ taken\ (s)}$

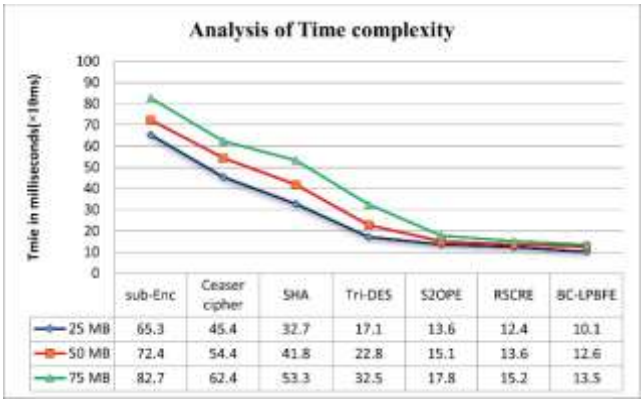

Figure 10 Comparison of time complexity

Figure 10 shows the various file size to handle the encryption at the meantime of evaluation by dissimilar methods, and the proposed system BC-LPBFE provides the least mean time of 13.6 ms as well as the previous cipher policy. This implementation had much-improved performance compared to prior methods.

Frequent occurrence state (FS) = $\frac{Repeated\ block\ of\ the\ cipher}{Total\ number\ of\ cipher\ block\ occurrence}$

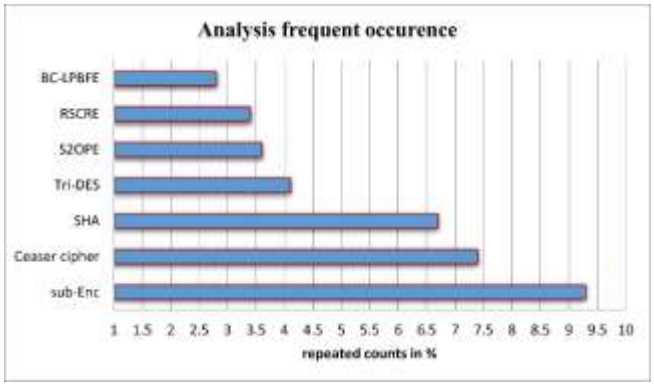

Figure 11: Comparison of frequent occurrence

The above Figure 11 shows the impact of execution at the frequent evaluation of lower complexity by different methods. The projected BC-LPBFE method proves the least failure state in 3.6 % which is the best evaluation to do the process quicker than other methods.

Table 3: Frequent occurrence rate

methods	A frequent occurrence in %		
	25 MB	50 MB	75 MB
sub-Enc	9.3	72.4	82.7
Ceaser cipher	7.4	54.4	62.4
SHA	6.7	41.8	53.3
Tri-DES	4.1	22.8	32.5
S2OPE	3.6	15.1	17.8
RSCRE	3.4	12.4	14.1
BC-LPBFE	2.8	8.3	10.2

Table 3 shows the frequent occurrence states to do the encryption whether data is encrypted during non-redundant evaluation with dissimilar methods. This shows that the implementation of the proposed crypto method has produced an active redundant frequent occurrence than previous methods.

.

5. Conclusion

Blockchain is a very powerful tool for applying data security and integrity on cloud platforms. To test the performance with simulated user accounts to modulate the data in Blockchain type depends on the user and ownership policy along with our data protection application. Timestamp Hashtag-based blockchain security using Lattice Verified Pair-block Folding Encryption (BC-LPBFE) for improving integrity proofing in the cloud environment. The proposed system produces 96.8 %

higher security performance than previous methods and lasting integration with Peer Verification Security based on lattice-based access control. Blockchain security on the cloud is still exploring the availability of concrete data and improves security in integrity applications.

References

1. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-based data preservation system for medical data,” Journal of Medical Systems., vol. 42, no. 8, pp. 141–153, 2018.
2. Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, “TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain,” IEEE Access., vol. 6, pp. 31077–31087, 2018.
3. L. Chen, Y. Li, H. Wen, W. Lei, W. Hou, and J. Chen, "BlockChain Based Secure Scheme For Mobile Communication," 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 2018, pp. 1-2, DOI: 10.1109/CNS.2018.8433155.
4. G. Liu et al., "A Program Behavior Study of Block Cryptography Algorithms on GPGPU," 2009 Fourth International Conference on Frontier of Computer Science and Technology, Shanghai, China, 2009, pp. 33-39, doi: 10.1109/FCST.2009.13.
5. J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems., vol. 22, no. 7, pp. 1214–1221, 2011
6. R. Kochan et al., "Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code," 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Dortmund, Germany, 2020, pp. 1-9, doi: 10.1109/IDAACS-SWS50031.2020.9297102.
7. J. Li, Q. Yu, Y. Zhang, and J. Shen, “Key-policy attribute-based encryption against continual auxiliary input leakage,” Information Sciences., vol. 470, pp. 175–188, 2019
8. S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” IEEE Access., vol. 6, pp. 38437–38450, 2018.
9. N. Kumar S. and M. Dakshayini, "Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology," 2020 International Conference on Mainstreaming BlockChain Implementation (ICOMBI), Bengaluru, India, 2020, pp. 1-5, DOI: 10.23919/ICOMBI48604.2020.9203442.
10. F. Gong, D. Li, N. Han, and S. Tian, "A Highly Trusted Demand Response System Based on Block-Chain," 2020 Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, 2020, pp. 1024-1027, DOI: 10.1109/AEEES48850.2020.9121488.
11. H. Wang and Y. Song, “Secure cloud-based EHR system using attribute-based cryptosystem and blockchain” Journal of Medical Systems., vol. 42, no. 8, pp. 152–160, 2018
12. S. V., A. Sarkar, A. Paul and S. Mishra, "BlockChain Based Cloud Computing Model on EVM Transactions for Secure Voting," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 1075-1079, doi: 10.1109/ICCMC.2019.8819649.
13. Saha and C. Srinivasan, "White-Box cryptography-based data encryption-decryption scheme for IoT environment," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 637-641, DOI: 10.1109/ICACCS.2019.8728331.
14. R. Yu et al., "Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network," in IEEE Access, vol. 5, pp. 24944-24951, 2017, DOI: 10.1109/ACCESS.2017.2767285.
15. S. A. Kalamsyah, A. M. Barmawi and M. Arzaki, "Digital Contract Using Block Chaining and Elliptic Curve Based Digital Signature," 2018 6th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2018, pp. 435-440, DOI: 10.1109/ICoICT.2018.8528771.
16. Y. Yao, L. Chu, L. Shan, and Q. Lei, "Supply Chain Financial Model Innovation Based on Block-chain Drive and Construction of Cloud Computing Credit System," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 2020, pp. 249-255, DOI: 10.1109/SmartIoT49966.2020.00044.
17. D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat and L. Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 2017, pp. 458-467, doi: 10.1109/CCGRID.2017.111.
18. B. Ravishankar, P. Kulkarni, and M. V. Vishnudas, "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments," 2020 International Conference on Mainstreaming BlockChain Implementation (COMBI), Bengaluru, India, 2020, pp. 1-4, doi: 10.23919/ICOMBI48604.2020.9203500.
19. C. Xu, K. Wang and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," in IEEE Cloud Computing, vol. 4, no. 6, pp. 50-59, November/December 2017, doi: 10.1109/MCC.2018.1081060.
20. L. Zhou, A. Fu, J. Feng, and C. Zhou, "An Efficient and Secure Data Integrity Auditing Scheme with Traceability for Cloud-Based EMR," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148673.
21. C. Wang, S. Chen, Z. Feng, Y. Jiang and X. Xue, "Block Chain-Based Data Audit and Access Control Mechanism in Service Collaboration," 2019 IEEE International Conference on Web Services (ICWS), Milan, Italy, 2019, pp. 214-218, doi: 10.1109/ICWS.2019.00044.
22. Y. Qu et al., "Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5171-5183, June 2020, doi: 10.1109/JIOT.2020.2977383.
23. M. Poongodi, M. Hamdi, V. Varadarajan, B. S. Rawal and M. Maode, "Building an Authentic and Ethical Keyword Search by applying Decentralised (Blockchain) Verification," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM

WKSHPS), Toronto, ON, Canada, 2020, pp. 746-753, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162859.
24. Y. Zhang, C. Xu, N. Cheng, H. Li, H. Yang and X. Shen, "Chronos$^{{\mathbf +}}$+: An Accurate Blockchain-Based Time-Stamping Scheme for Cloud Storage," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 216-229, 1 March-April 2020, doi: 10.1109/TSC.2019.2947476.
25. J. Wang, J. Mu, S. Wei, C. Jiang and N. C. Beaulieu, "Statistical Characterization of Decryption Errors in Block-Ciphered Systems," in IEEE Transactions on Communications, vol. 63, no. 11, pp. 4363-4376, Nov. 2015, doi: 10.1109/TCOMM.2015.2474860.
26. W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi and H. Hui, "Cryptographic Primitives and Design Frameworks of Physical Layer Encryption for Wireless Communications," in IEEE Access, vol. 7, pp. 63660-63673, 2019, doi: 10.1109/ACCESS.2019.2914720.
27. X. Fu, H. Wang and Z. Wang, "Research on Block-Chain-Based Intelligent Transaction and Collaborative Scheduling Strategies for Large Grid," in IEEE Access, vol. 8, pp. 151866-151877, 2020, doi: 10.1109/ACCESS.2020.3017694.
28. K. Xue et al., "A Secure, Efficient, and Accountable Edge-Based Access Control Framework for Information-Centric Networks," in IEEE/ACM Transactions on Networking, vol. 27, no. 3, pp. 1220-1233, June 2019, doi: 10.1109/TNET.2019.2914189.
29. J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," in IEEE Access, vol. 4, pp. 9239-9250, 2016, doi: 10.1109/ACCESS.2016.2645904.
30. R. Viswanathan, D. Dasgupta and S. R. Govindaswamy, "Blockchain Solution Reference Architecture (BSRA)," in IBM Journal of Research and Development, vol. 63, no. 2/3, pp. 1:1-1:12, March-May 2019, doi: 10.1147/JRD.2019.2913629.
31. J. R. Teja, "Proposing method for Public record maintenance using Block chain," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India, 2020, pp. 1-5, doi: 10.23919/ICOMBI48604.2020.9203162.
32. S. Liu and S. He, "Application of Block Chaining Technology in Finance and Accounting Field," 2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), Changsha, China, 2019, pp. 342-344, doi: 10.1109/ICITBS.2019.00090.
33. M. S. Christo, A. M. A., P. S. G., P. C. and R. K. M., "An Efficient Data Security in Medical Report using Block Chain Technology," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0606-0610, doi: 10.1109/ICCSP.2019.8698058.
34. J. K. Pal and J. K. Mandal, "A random block length based cryptosystem through multiple cascaded permutation-combinations and chaining of blocks," 2009 International Conference on Industrial and Information Systems (ICIIS), Peradeniya, Sri Lanka, 2009, pp. 26-31, doi: 10.1109/ICIINFS.2009.5429895.
35. S. Yunling and M. Xianghua, "An Overview of Incremental Hash Function Based on Pair Block Chaining," 2010 International Forum on Information Technology and Applications, Kunming, China, 2010, pp. 332-335, doi: 10.1109/IFITA.2010.332.
36. Y. Rui-jun, H. Jin-bo and C. Yan, "Design of data sharing module based on medical block chain," 2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Shanghai, China, 2019, pp. 149-152, doi: 10.1109/ICIIBMS46890.2019.8991529.
37. N. Savitri, A. W. S. B. Johan, F. Al Islama A and F. Utaminingrum, "Efficient Technique Data Encryption with Cipher Block Chaining and Gingerbreadman Map," 2019 International Conference on Sustainable Information Engineering and Technology (SIET), Lombok, Indonesia, 2019, pp. 116-119, doi: 10.1109/SIET48054.2019.8986084.
38. T. Teerakanok and S. Kamolphiwong, "Accelerating asymmetric-key cryptography using Parallel-key Cryptographic Algorithm (PCA)," 2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Chonburi, Thailand, 2009, pp. 812-815, doi: 10.1109/ECTICON.2009.5137170.
39. J. Moubarak, E. Filiol and M. Chamoun, "On blockchain security and relevant attacks," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, 2018, pp. 1-6, doi: 10.1109/MENACOMM.2018.8371010.