isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,Apr,2023 ,ISSN_NO: 2321-3337

# TIME ENABLING METHOD TO APPROACH TO SECURE DATA BASED ON BLOCKCHAIN

**Indra.V[1], Jayaramya.E[2], Nivetha.V[3], Malathi.S[4]**

UG Scholar[1 2 3] –Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, India.

Assistant Professor[4]- Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, India.

indravd0308@gmail.com, jayaramya127@gmail.com, nivethacsc.2020@gmail.com. malathi.s@grt.edu.in

***Abstract*** - There are several research works focusing on preserving the privacy of the electronic healthcare record company. We propose a proxy Blowfish encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while blowfish encryption construction will grant legitimate users access to the data. we design an inference attack-resistant e-healthcare cloud system with fine grained access control. We first propose a three-layer encryption scheme. To ensure an efficient and fine-grained access control over the company data. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. This Technique will allow only limited access rights to an authorized agent to access the records for a specific time period. This technique will use a searchable encryption technique. Process of design applications with this method is through several stages, such as process of encryption, decryption, key generation and testing of the methods used. To reduce the storage problem in Cloud we have split the file into different block and get stored, so storage problem get rectified. By using those methods and algorithm our company Data can share privacy and secure. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security.

## 1. INTRODUCTION

This technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy It allows the users to on-demand rent the storage resources in cloud with usage-based pricing, and remotely access their data at any time and from anywhere [1]. One fundamental aspect of this paradigm shifting is to centralize the data from the users' infrastructure to the cloud. Users can acquire almost unlimited storage capability from the cloud, and their cost for infrastructure purchase. and storage maintenance can be released. Although storing data remotely to the cloud brings appealing benefits to users, it also brings new challenging security threats towards users' outsourced data.

## 2. OVER VIEW OF BLOWFISH ALGORITHM

The Blowfish algorithm has many names, including Blowfish encryption, Blowfish cipher, or others, but they all have the same meaning and function. So let's talk about the Blowfish algorithm and try to find one true definition. Once the Blowfish algorithm got included in several cipher suites and encryption products, vulnerabilities were found. Schneider worked on these vulnerabilities and made a better and more reliable encryption called AES. We completely support the statement that without the development of the Blowfish algorithm, there won't be AES or other symmetric encryption techniques used today to keep our computers safe from online attacks. Once the Blowfish algorithm got included in several cipher suites and encryption products, vulnerabilities were found. Schneider worked on these vulnerabilities and made a better and more reliable encryption called AES. We completely support the statement that without the development of the Blowfish algorithm, there won't be AES or other symmetric encryption techniques used today to keep our computers safe from online attacks.

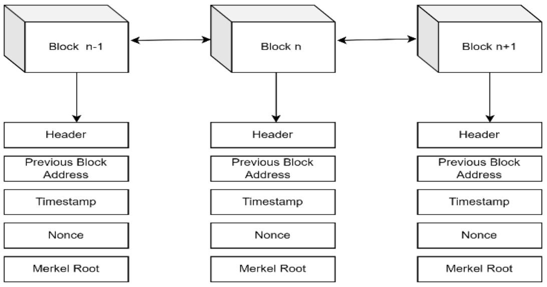


**Fig.1.1 Blowfish Algorithm**

## 2.1 CHARACTERISTICS OF BLOWFISH ALGORITHM

**1.Data encryption**

Data encryption happens through a 16-round Feistel network, with each round consisting of a keydependent permutation and a key- and data-dependent substitution. Large, key-dependent S-boxes work with the substitution method and form an integral part of the data encryption system in Blowfish. All encryption operations are XORs -- a type of logic gate -- and additions on 32-bit words.

**2. Key expansion and subkeys** In the key expansion process, maximum size 448-bit keys are converted into several subkey arrays totaling 4,168 bytes. Subkeys form an integral part of the Blowfish algorithm, which uses a large number of them. These subkeys are precomputed before encryption or decryption can take place.

In Blowfish, the P-array consists of 18 32-bit subkeys and four 32-bit S-boxes with 256 entries each. The subkeys are calculated as follows:

- The P-array and S-boxes are initialized with a fixed string of hexadecimal digits of pi.
- The first element in the P-array (P1) is now XORed with the first 32 bits of the key, P2 is XORed with the second 32-bits and so on, until all the elements in the P-array are XORed with the key bits.
- All-zero strings are encrypted by the algorithm as described in the above steps.
- P1 and P2 arrays are replaced with the output from step 3 above.
- This output is encrypted by Blowfish with modified subkeys.
- The output of step 5 modifies P3 and P4 in the P-array.
- This process continues until all the P-arrays and four S-boxes are modified.

## 2.2. BLOWFISH ALGORITHM

Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use.

- blockSize: 64-bits
- keySize: 32-bits to 448-bits variable size
- number of subkeys: 18 [P-array]
- number of rounds: 16
- number of substitution boxes: 4 [each having 512 entries of 32-bits each]

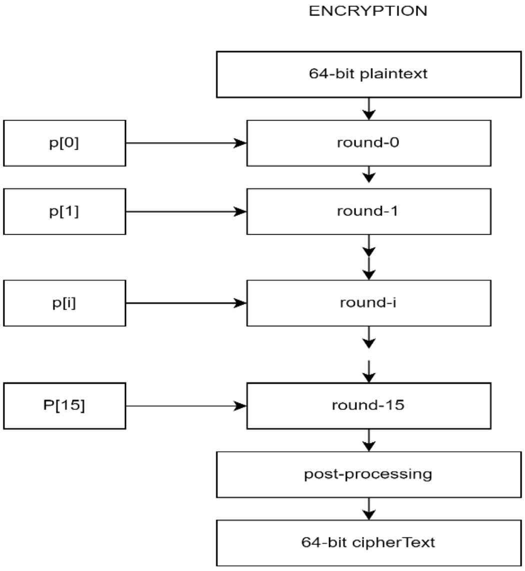
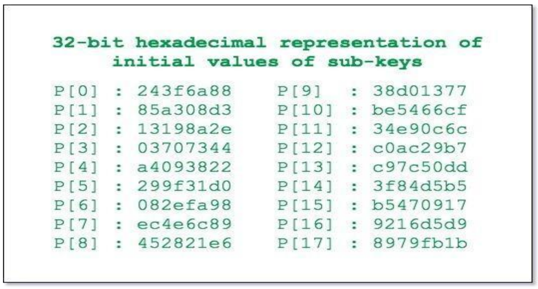


**Fig.2.1 Encryption**

**Step1: Generation of subkeys:**

- 18 subkeys {P[0]….P[17]} are needed in both encryption as well as decryption process and the same subkeys are used for both the processes.
- These 18 subkeys are store in a P-array with each array element being a 32-bit entry.
- It is initialized with the digits of pi(?).
- The hexadeccimal representation of each of the subkeys is given by



```
32-bit hexadecimal representation of
      initial values of sub-keys

P[0] : 243f6a88     P[9]  : 38d01377
P[1] : 85a308d3     P[10] : be5466cf
P[2] : 13198a2e     P[11] : 34e90c6c
P[3] : 03707344     P[12] : c0ac29b7
P[4] : a4093822     P[13] : c97c50dd
P[5] : 299f31d0     P[14] : 3f84d5b5
P[6] : 082efa98     P[15] : b5470917
P[7] : ec4e6c89     P[16] : 9216d5d9
P[8] : 452821e6     P[17] : 8979fb1b
```

**Fig.2.2 hexadecimal representation of initial value of sub-keys**

- Now each of the subkeys is changed with respect to the input key

The resultant P-array holds 18 subkeys that is used during the entire encryption process.

**Step2: Initialise Substitution Boxes:**

- 4 Substitution boxes (S-boxes are needed{S[0]….S[4]} in both encryption as well as decryption process with each S-box having 256 entries {S[i][0] …. S[i][255],0&lei&le4} where each entry is 32-bit.
- It is initialized with then digits of pi(?) after initializing the P-array.

**Step3: Encryption:**

a) The encryption function consists of two parts:

**a) Rounds:**

The encryption consists of 16 rounds with each round(Ri) taking inputs the plain Text(P.T.) from previous round and corresponding subkey(Pi).The description of each round is as follows:

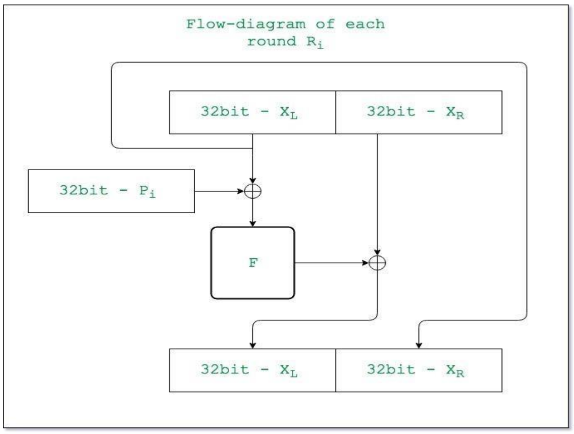


**Fig.2.3 flow diagram for each round**

The description of the function "F" is as follows:

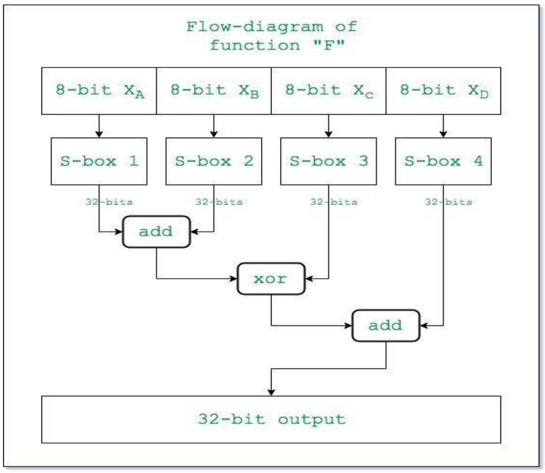


**Fig.2.4 flow diagram of function "F"**

Here the function "add" is addition modulo 2^32.

b) Post-Processing: The output after the 16rounds is processed as follows:

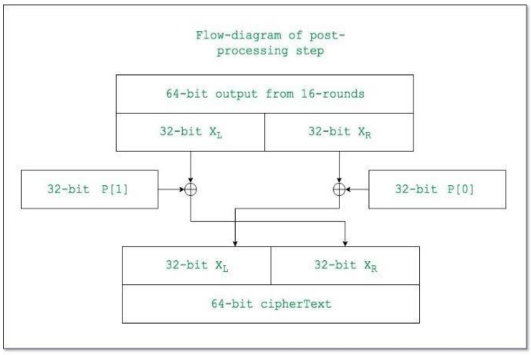


**Fig.2.5 flow diagram of post processing step 3.**

## EXISTING SYSTEM

In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-andencrypt solution means the data owner has to be online all the time, which is practically not feasible.

The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users A proxy runs the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no idea of the data owner's secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data-sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties.

### 3.1. DISADVANTEGS OF EXISTING SYSTEM

1. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users.
2. Existing schemes adopt the conventional ciphertext policy proxy re encryption to encrypt which inevitably expose the access policy to the cloud.
3. the data attributes while preserving the sta_tistical data of the role attributes is a challenging problem.
4. Attract can they have chance to attack the file form cloud.
5. In addition to the above, PRE has been used to mitigate security problems in Cloud.

## 4. PROPOSED SYSTEM

To ensure an efficient and time enable proposed for file storage. the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the Cloud, we further construct a blind data retrieving protocol. We provide rigorous security analyses and conduct extensive experiments to confirm and efficiency of our proposed schemes. We include Blowfish algorithm for file storage.file encryption Our proposed scheme should control the privacy protection to a specific level. We measure the privacy disclosure of our scheme by the attacker's confidence in the success of an attack. our proposed scheme, and show that the security and privacy goals have been achieved. We first prove that the three-layer encryption scheme. We proposed. we proposed finegrained access control over the Company data.

### 4.1. ADVANTEGS OF PROPOSED SYSTEM

1. our proposed scheme, and show that the security and privacy goals have been achieved. We first prove that the three-layer encryption scheme is secure.
2. We provide rigorous security analyses and conduct extensive experiments to confirm the efficacy and efficiency of our proposed scheme blowfish enryption.
3. Uses attributes of the users to provide access to data. Time enabled method specifies time for every attribute of a user which is termed as access time of the attribute.
4. The key problems of this approach include establishing access control for the encrypted data
5. The files are storing in randomized folder to protect form attacker

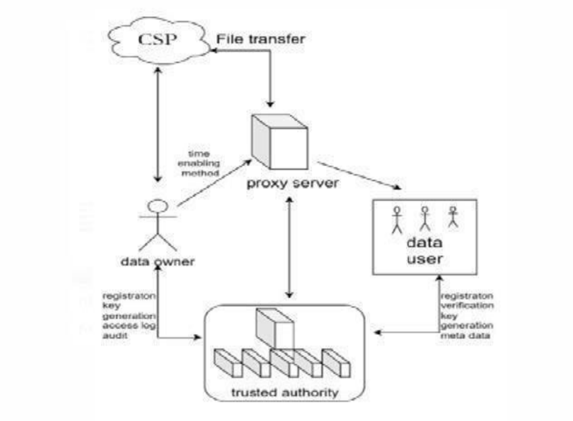
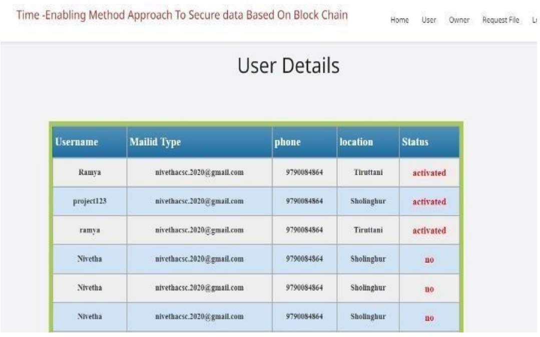

CSP
File transfer
time enabling method
proxy server
data owner
data user
registraton key generation access log audit
registraton verification key generation meta data
trusted authority

**Fig.4.1 Proposed System**

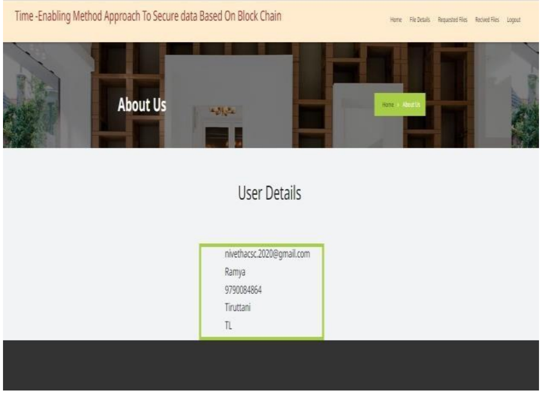
## 5.EXPERIMENTAL RESULTS


Time -Enabling Method Approach To Secure data Based On Block Chain

User Details

| Username | Mailid Type | phone | location | Status |
|---|---|---|---|---|
| Ramya | nivethacsc.2020@gmail.com | 9790084864 | Tiruttani | activated |
| project123 | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | activated |
| ramya | nivethacsc.2020@gmail.com | 9790084864 | Tiruttani | activated |
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | no |
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | no |
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | no |

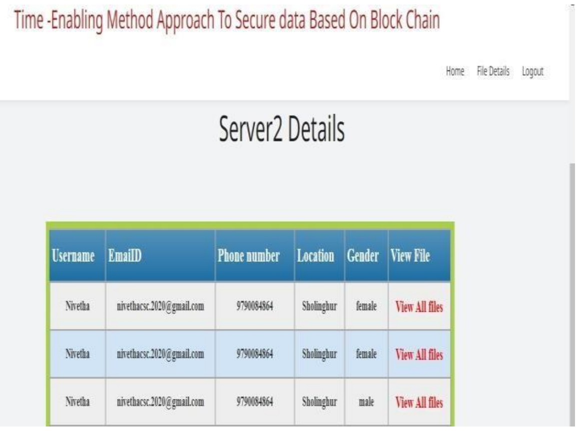
**Fig.5.1 Shows User Details**



User Details

nivethacsc.2020@gmail.com
Ramya
9790084864
Tiruttani
TL

**Fig.5.2 Shows user authentication**


Time -Enabling Method Approach To Secure data Based On Block Chain
Home
File Details
Logout

Server2 Details

| Username | EmailD | Phone number | Location | Gender | View File |
|---|---|---|---|---|---|
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | female | View All files |
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | female | View All files |
| Nivetha | nivethacsc.2020@gmail.com | 9790084864 | Sholinghur | male | View All files |

**Fig.5.3 Shows server details**

## 6. CONCLUSION

We first propose a Time enable and blowfish encryption scheme. we propose to define a specialized access policy for each data attribute in the Company, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute. To preserve the access pattern of the data attributes in the, we construct a blind data retrieving protocol based on the Paillier encryption. provides the encryption module for the re-encryption and also time privileges for accessing particular file. we present a block chain based system model that allows for flexible authorization on encrypted data. Fine grained access control is achieved, and it can help data owners achieve privacy preservation The proposed scheme ensures data confidentiality and integrity against the cloud server. During the auditing process, the TPA can verify the correctness of the proof without decrypting it and without key exposure. Security and performance analysis shows that the proposed scheme requires minimal extra computation while guaranteeing data privacy and integrity.

## 7. REFERENCE

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347– 2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K.Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp. 5– 6.

[6] D. Balfanz et al., “Secret handshakes from pairing-based key agreements,” in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

[7] R. Canetti, S. Halevi, and J.Katz, “Chosen cipher text security from identity-based encryption,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207– 222.

[8] T. Koponen et al., “A data-oriented (and beyond) network architecture,” in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181–192.

[9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, “Developing information networking further: From PSIRP to pursuit,” in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, “Secure naming for a network of information,” in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops,2010, pp. 1–6.

[11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, “A routing scheme for content-based networking,” in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.

[12] I. Psaras, W. K. Chai, and G. Pavlou, “ Probabilistic in-network caching for information centric networks,” in Proc. 2nd ed. ICN Workshop Inform.- Centric Netw., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., “Trace-driven analysis of ICN caching algorithms on videoon-demand workloads,” in Proc. 10th ACM Int. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363–376.