Securing Data in Decentralized Cloud Storage Using Blockchain

Rohini Pise and Sonali Patil

November 27, 2020

Securing Data in Decentralized Cloud Storage using Blockchain

Mrs. Rohini G. Pise, Assistant Professor IT Department, Pimpri Chinchwad College of Engineering

Dr. Sonali Patil, Professor IT Department, Pimpri Chinchwad College of Engineering

Abstract:Now a day's large amount of data is stored on cloud storage which is required to be protected from the unauthorized users. To maintain the privacy of data various algorithms are used to protect data so that data can be provide (CIA) confidentiality, integrity, accessibility. However, the existing of centralized cloud storage lacks to provides these CIA properties. So, to enhance the data storing technique(DCS) decentralized cloud storage is used and with the help of blockchain technology it is effectively helps to protect data from tampering or deleting a part of data. For any kind of data blockchain stores it in number of blocks which are linked in continuous order through hash value in order to reduce the chances of data altering. For this purpose, SHA-512 algorithm is use to implement the blockchain technology, because it works on hashing function when data is given to its input. Hashing algorithm used in many aspects where security of data is required such as message digest, password verification, digital certificates or even a blockchain. By the combination ofthesemethods makes data more secure and reliable to user who access data which is store on cloud storage. However, with the help of various algorithms we enhance the security of data by encryption. In this paper (AES) Advance Encryption Standard is used to encrypt and decrypt the data due to significant features of this algorithm.

Keywords—CIA, Decentralized Cloud Storage,SHA-512, Advance Encryption Standard, Encrypt, Decrypt.

I.INTRODUCTION

Now a day's cloud storage is used to store and retrieve data which is based on internet, instead of local storage devices for more reliable, secure and availability of data. But data is very important and should not be reveal to any unauthorized person, for this purpose encryption method is used to convert this plain data in cipher text and decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm plays most important role to make data more secure. To achieve these operations some mathematical calculations are made and it is also possible to explain them practically. This operation provides CIA properties for data and assure that data will remain secure and original. To encrypt and decrypt, data will be divided into chunk of block while performing this operation, there are various algorithm also available which are categorized in two different types. First one is symmetric encryption method, in which data can be encrypt and decrypt with same key. After performing the encryption method data is converted into unreadable form, to get the original message back intended user must have key which is used while encryption process. Then this method reverses its process and data will available in understandable form. Second one is asymmetric encryption method, where two keys are generated, one for encryption and second for decryption.Advance Encryption Standard (AES) is also known as Rijndael algorithm which works up to 128 bits of block length. This algorithm allows key length of three different bits which is 128, 192, 256 bits. To convert plain text into cipher, this encryption is dependent on key length where this algorithm repeats its method several times called rounds to enhance the security of data. For 128 bits it uses 10 rounds, for 192 bits it uses 12 rounds and for 256 bits it uses 14 rounds. Excepting the last round in every case, rest of the rounds are equal to each other. After performing this operation on data encrypted data block is obtained, which is in unreadable form. To get the original data back the reverse procedure of AES algorithm is required perform on encrypted data.

While after performing study in depth by the researcher on AES algorithm there is an evidence that there are several aspects which suffers from vulnerabilities and needs attention to refine the level of security are given as follows.

i) Most of the researchers have been notice that increasing number of rounds will helps in increasing security of data block.

ii) AES algorithm is developed to work with 32-bits, that's why it is not work with 64-bit.

iii) Process of deciphering is slower than the process of enciphering.

iv) Addition of last round excluding mix-column have no benefit in increasing security, insertion and deletion of it can be no effect on security stated by authors of AES.

v) Encryption and Decryption process of thousands of bits require different time because of repetitions of many rounds.

II.RELATED WORK

In traditional cloud storage where all data is store at only oneplace called centralized cloud storage, the chances of data security is less as compared to decentralized cloud storage due to owner of centralized cloud could monitor the data and it can be altered or theft. With quick requirement to access data each individual wants to retrieve their data instantly and more securely for this reason decentralized cloud storage is developed. In decentralized cloud storage data is stored in more than one place, this itself reduce the chances of data reaching to the data stealers. Because data stealers unaware of where the rest of the data is stored, due to this reason decentralized cloud storage is popular and used widely. The main objective of DCS is to provide independent data nodes with security and availability of data.

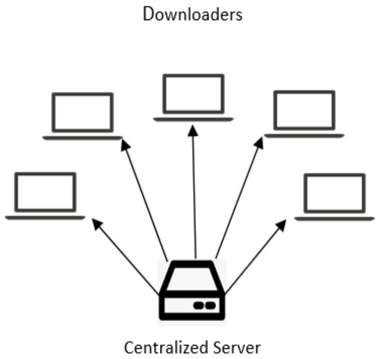


Figure 1: Traditional Centralized Cloud Storage [1]

As shown in Figure 1 all data user who wants to access their data is dependent on only one server. Due to this bottleneck can arises and results in longer time needed to access data because high load on single point server. There is also limited numbers of user who can connect the server at same time, the application where many numbers of user needs to connects and access server is not possible, and if this server caught by some hardware failure or by some fault in setup, the data stored on server will be inaccessible. If this kind of situation occurs and data may unexpectedly lose then it is very difficult to retrieve data back.The maintenance of this server is also high. Another issue with this data storing technique is that they charge highest possible price to their customer to use their services. Due to overcome these all the situations faced in centralized cloud storage, decentralized cloud storage is used to remove all the difficulty which are faced in centralized structure.

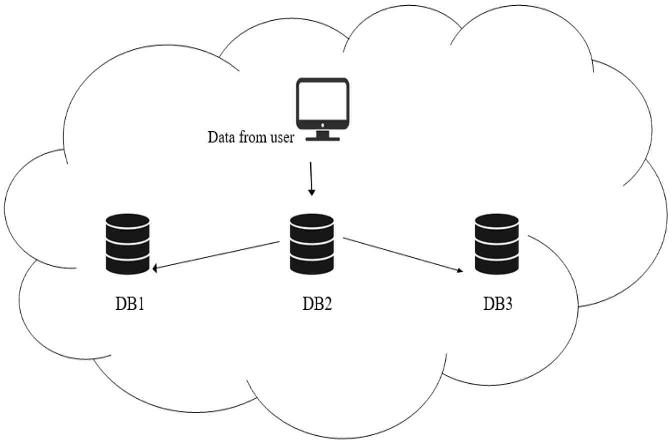


Figure 2: Decentralized Cloud Storage [1]

The structure of decentralized cloud storage is shown in figure 2. Data from user is being stored on multiple database assign by server to make replica of data, while storing data on different server it is breaks into piece of chunks. This means, there is huge storage space to store data and cost for storing data on cloud server is less. There is no single party to own the data and control over it. Another advantage of decentralized cloud storage is that these are continuously live network for accessible of data any time. This method of storing data is helpful when hackers want to steal data stored on cloud storage. Because of this, they won't able to retrieve complete data. As data stored data at different location is itself secure in senses of data lose but to protect data from hackers, we need encryption method to make data more secure. Even a single data file is stored at multiple location with small data blocks, but what if that small block of file contains sensitive information. For this reason, we need encryption method to encrypt data. All these cloud storage uses some sort of algorithm to make data more secure for their customers.Siacoin, Filecoin, Storj, Maidsafe are some service provider of decentralized cloud storage. As decentralized cloud storage works on blockchain technology it is far more secure than centralized cloud storage with respect to data security. Even hacker able to access a piece of data, due to encryption mechanism used by the service providers hackers are unable to decrypt the information within data block. That's why decentralized cloud storage is preferred as compared to centralized cloud storage structure. [1]

To implement such secure system, we are using Advance Encryption Standard to make data more secure and keep data out of reach from the attackers.

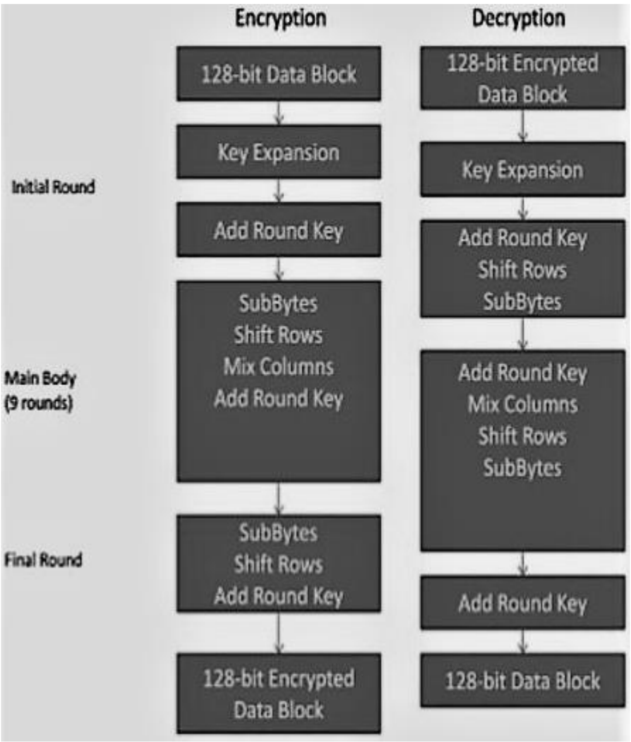


Figure 3: AES Algorithm structure [2]

i) Data Block: In this first stage, data is divided into separate blocks. As shown in figure 3 data is divided into columns of four by four in sixteen bytes.

ii) Key Expansion: This process involves in taking the words as initial key and create array of 44 words, then use with series of keys for every next round for encryption process.

iii) Add Round Key: Key expansion is done to make 10 keys by method called key schedule. This is done with XORing with resulted data to make input for the next round.

iv) Substitute bytes: Here, whole words are coded in such a way that one letter after of current word in alphabet. For example, hello changes to ifmmp.

v) Shift Rows: As name give idea for this concept, each next row is moved one row back means second row is shift in space of first row, third row is shift in space of second row and so on.

vi) Mix Columns: Each column has some value which is given by the previous stages of algorithm. Likewise, this mixing of column is performed.

vii) Add Round Key (again): This block takes input from previous block and add round key which are derived at the beginning of encryption.

At the end of this steps, we get encrypted data. To get the original data back reverse operation of encryption is performed on encrypted data and resultant data would be our original data. [2]

Now while uploading encrypted data on the cloud server to keep track of sequence of uploaded data blockchain technology is used. Blockchain technology is technique which records the information is such way that it is impossible to interchange the system transaction of data. It works on hash function. Each block of data is linked with next block of data by hash value. There is no concept of encryption and decryption in blockchain, that's why once some operation is performed on data it cannot be reversed. For this purpose, blockchain technology is used and considered most trustworthy, appended only and efficient for application where logs of data are more important. Such application including banking, online music, Internet of things (IoT). This eliminates the requirement of third party to validate the transactions for peer-to-peer network. It was invented by a Japanese fellow called Santoshi Nakamoto and started using it in 2008.

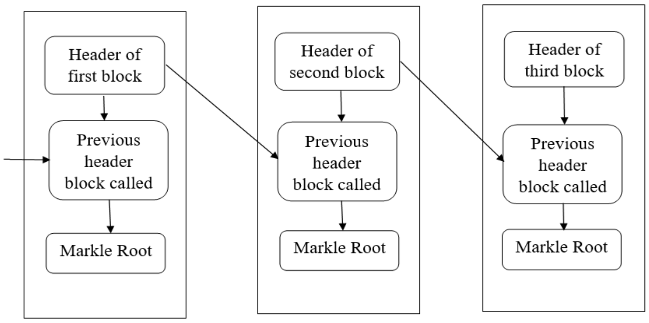


Figure 4: Structure of Blockchain [3]

As shown in Figure 4 blocks of data are linked to each other in chronological way. Header block contains the information about which is the next block to append. After linking to the block of data, the header of first block is called hash block. This sequence of block is kept in markle root block and all the information related transaction is kept secure in this block. This kind of architecture refers to store the data in the form of block and in digital manner. It also helps to keep detail control over processing and transactions without having the central point. By having such structure removes cheating, stealing the data attacks or other cyber-crime attack. [3]

To implement chain of blocks we need some sort of hashing method which keeps the data in sequence by their updating order. Means first transaction made on data remains at first, second transaction made on data remains at second and so on. By doing this we actually achieving such transaction of data or chain of block in which alteration is impossible. One more thing is achieved using blockchain technology, which data repetition is not possible. This reduces the unrequired or duplication of data blocks. For this purpose, we are using SHA-512 hashing algorithm.

SHA-512 algorithm is a hashing algorithm which perform on data in one-way and it is developed by Ron Rivist. It is an evolution of previous algorithms such as SHA 0, SHA 1, SHA 256, SHA 384. Hashing is also known as compression or message summary functionwhich takes the entire variable length and change it into a binary sequence of fixed length. This hash function is designed in such way that it is impossible to reverse the process, hence it is called one direction. The concept of hashing algorithm is shown in Figure 5.

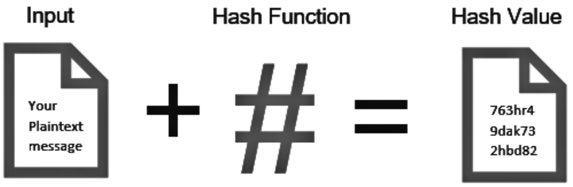


Figure 5: Working ofhashing algorithm [4]

Working of SHA-512 algorithm is given as follows:

The first step is to adding a bit as per algorithms rules. It is basically first step in all the algorithms. Then SHA-512 algorithm process block of message in block of 1024 size. The next step is to adding bits again with original message, the addition of bits in message is of 128-bits. SHA-512 is a construction where data is absorbed into sponge andthen the output is derived as a squeezed from the input. In the absorbing stage data is XORed and in squeezing stage data is altered with state transformation.

SHA-512 is similar in structure of SHA-256 but there are some variation in some aspects such as i) Message is divided into 1024- bit of chunks ii) Initial hash value and rounds are extended up to 64-bits iii) Instead of 64 rounds there are 80 rounds iv) Round constant based on starting first 80 primes. v) word size is used for computation is 64 bits long vi) Fixed length of message is 128-bits long vii) Shifting and Rotation rounds are different. According to these points the structure of SHA-512 is appears like in Figure 6.

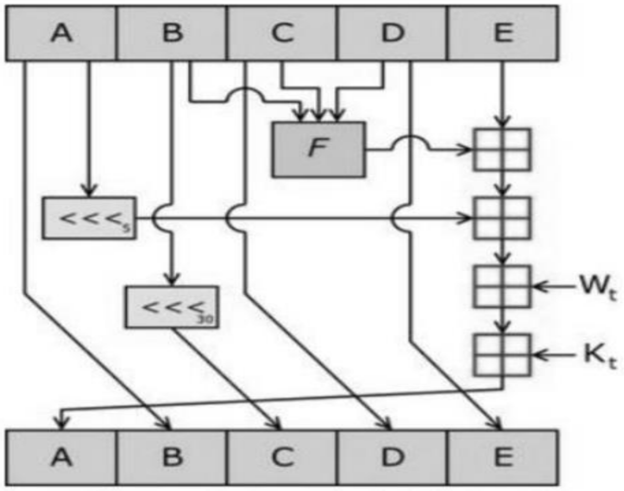


Figure 6: Structure of SHA-512 [4]

With the help of AES and Hashing algorithm we have design an architecture where user upload data to cloud server and with the help of private key the receiver is able to retrieve that data. [4]

III.PROPOSED SYSTEM

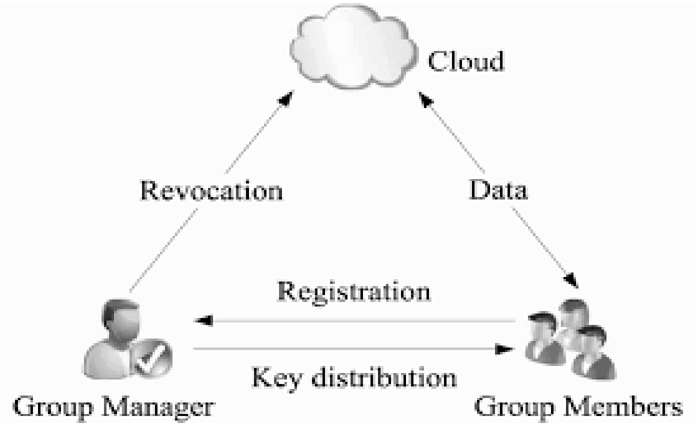


Figure 7: System Model [5]

In the proposed model the data owner store data on cloud server. Cloud server is always remaining an attractive point for intruder to steal the valuable data. For security purpose a key is shared by owner to data user to access that data. To make that data unreadable to intruder AES algorithm is used. So, intruders are not able to steal the data. With the help of hashing algorithm SHA-512 data blocks are linked to each other and if data blocks are found to be missing, we have developed a system which data user is able to know which data block is attacked by the hackers.

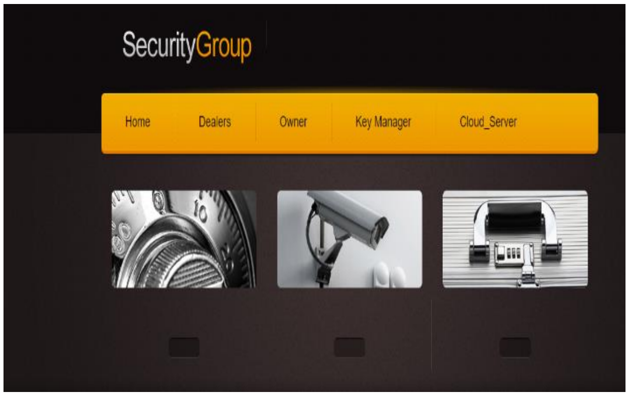
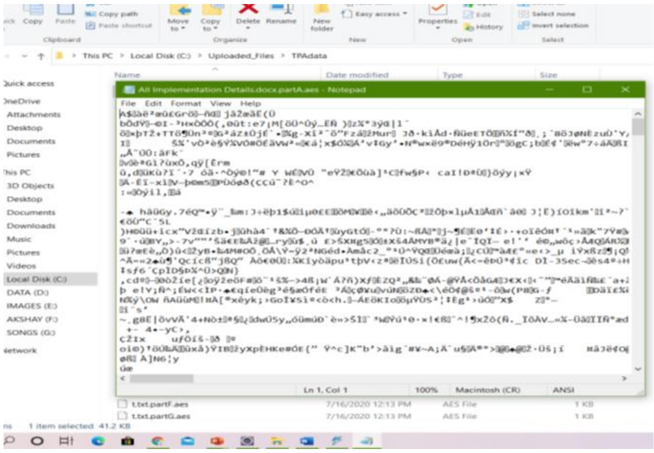


Figure 8: Screenshot 1

As shown in above figure there are four main modules which are dependent on each other. There are also sub-modules which are dependent on main as well as sub-modules. Data owner own the storage space on cloud server. The dealer(user) gives the required information of him to the owner. It's up to the owner to approve the request of user to use its services. Once the owner allows to use his services then user is able to store data on cloud server. In some cases, data owner charge data user to access his data which is stored on cloud server. Data stored on server have a key which is create when data stored on cloud server, so the user required that key to get that data. To access data which is stored on cloud server user needs to send request to Key Manager to access the file. If it denies to send private key then it is not possible to user to access and down load the file. All the users who wish to use data which is stored on cloud storage is require permission to access that data. Key Manager have the authority to share the key to respective user to access the data on cloud.

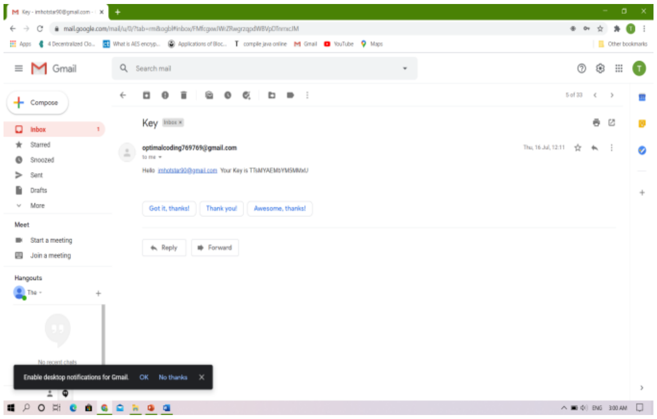


```
[illegible]
```

t.txt.partF.aes	7/16/2020 12:13 PM	AES File	1 KB
t.txt.partG.aes	7/16/2020 12:13 PM	AES File	1 KB

Figure 9: Screenshot 2

The encryption algorithm is used in this approach makes the data unreadable, that's why even in worst case some part of data is steal by user it is not possible to decrypt. It is not only the matter of reverse the encryption process to make it readable but the key when used at the time of encryption. The key must be the same which is used while encryption. This approach increases the security level in such architecture.

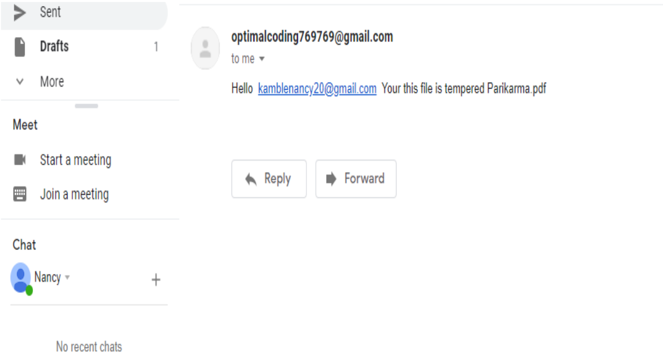


optimalcoding769769@gmail.com
to me

Hello imhotstar90@gmail.com Your Key is TTsMYAEMbYM5MMxU

Figure 9: Screenshot 3

To access the data on cloud server a key is shared by Key Manager to the user on registered details of user as shown in Figure 9.



optimalcoding769769@gmail.com
to me

Hello kamblenancy20@gmail.com Your this file is tempered Parikarma.pdf

Figure 10: Screenshot 4

If some modification on data is done by attackers then user is notified as per above way shown in Figure 10.

Observation of Required time to perform operation on data.

We have also measured the time required by AES algorithm to encrypt the data and time required to perform the hashing operation on data.

File Size in Kilobytes	AES(256)	SHA-512	Time in Miliseconds
12KB	6.6ms	20.595ms	27.195ms
25KB	12.3ms	37.370ms	49.67ms
5KB	2.77ms	9.040ms	11.81ms

Table 1: Required time to perform operation by algorithm

As per observation the time required to perform respective operation on data is dependent on system specification. The experiments are done by personal computer with a configuration of Intel (R) Core (TM) i5 – 8th Generation 8250U CPU @ 1.80GHz, 8GB RAM, Windows 10 64-bit operating system version 1909. We have also observed the time on systemwhich have less configuration than above mention, it required more time to perform operation.

IV. CONCLUSION

This paper suggests a secure and efficient way to store data on cloud. Blockchain-based cloud storage with data encryption gives data security in decentralized structure. The proposed model is suitable to implement the blockchain structure. The algorithms used to implement the system model is efficient and required less time and give high security for the data which is being stored on cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in data files of user for their benefits.

V. REFERENCES

[1]Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and VladimiroSassone - Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments, In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

[2]Ako Muhamad Abdullah - Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Article · June 2017, ResearchGate publication.

[3] Anita V. Mithapalli, Swati S. Joshi - A Framework for Secure Data Storage and Retrieval in Cloud Environment, ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019, International Journal of Engineering and Advanced Technology (IJEAT).

[4]MeilianaSumagita and Imam Riadi - Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 373-381 The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001.

[5]AkshayBabrekar, Prof. Rohini G. Pise - Public Key Encryption for Cloud Storage Attack using Blockchain, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-2, July 2020.

[6] Aradhana, Dr. S. M. Ghosh - Review Paper on Secure Hash Algorithm with Its Variants, DOI: 10.13140/RG.2.2.13855.05289, ResearchGate publication.

[7] Avdhut Suryakant Bhise, Phursule R.N. - A Review of Role based Encryption System for Secure Cloud Storage, International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 14, January 2015.

[8] Avdhut Suryakant Bhise, R. N. Phursule - Developing Secure Cloud Storage System by Integrating Trust and Cryptographic Algorithms with Role based Access Control, International Journal of Computer Applications (0975 – 8887) Volume 168 – No.10, June 2017.

VI. AUTHORS PROFILE

Mrs. Rohini G. Pise is currently working as an assistant professor in IT Department, Pimpri Chinchwad College of Engineering, Pune. Her area of research interest is Computer security, Information security, Internet of Things, Cryptography

Dr. Sonali D. Patil is currently working as an HOD of IT Department, Pimpri Chinchwad College of Engineering, Pune. Her area of research interest is Information Security, Blockchain Technology