IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 1, January 2020, ||Series -III|| PP 13-18

Blockchain Based Secrete Key And Transaction Storage System For Documents Stored On Cloud

Ms. Kaushiki Tapadiya, Mr. Krishna Gupta, Prof. Poonam Lohiya
Computer Science and Engineering Prof.Ram Meghe Institute of Technology and Research Amravati, India
Computer Science and Engineering Prof.Ram Meghe Institute of Technology and Research Amravati, India
Computer Science and Engineering Prof.Ram Meghe Institute of Technology and Research Amravati, India

Received 01January 2020; Accepted 15 January 2020.

Abstract: Cloud document storage is becoming very popular, cost efficient and secure nowadays. Though cloud is very cost-efficient storage, the documents are accessible to service providers. Many literatures are available for document security in cloud. In most of the literatures, document encryption technique is described using different algorithms. Encrypting documents before storage is a good idea, but if encrypted documents as well as the secrete keys both are maintained on cloud server only, there is a possibility of leakage as the cloud service provider is an honest but curious entity. So, it can be a big risk if we maintain documents as well as their keys on cloud. On the other hand, if we apply unbreakable encryption on documents before storing on cloud then the searching over documents will be critical. Therefore, in this paper we focus on cloud document security as well as searching over cloud documents using AES algorithm, Caesar algorithm and blockchain technology.

Keywords: Blockchain, Cloud Computing, Advanced Encryption Algorithm, Ceasar Algorithm, public key,transaction management

I. INTRODUCTION

Cloud security is a hottest research topic nowadays. Various literatures are available on document encryption on cloud to provide security to the documents stored on cloud. No doubt encryption plays a vital role in cloud security process, but on the other hand the one who knows encrypted document as well as key will be able to attempt for decryption. It seems that it is not enough to encrypt cloud documents, instead along with the encryption we have to keep keys away from documents securely. But as we know cloud refers to centralization, if we are considering cloud it is obvious that complete data is stored at one place. Therefore, to maintain secrete keys and documents separately, we proposed a new technique in which documents will be stored on cloud server and secrete keys will be maintain in blockchain.

A blockchain is originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block has a cryptographic hash of the previous block, a timestamp, and transaction data. This technology resists the modification of data. Blockchain refers to the storage of important transaction on distributed servers. Blockchain is generally used for bit coin related transaction management. There are three types of block chains; public, private and protected. The main difference between a private and public blockchain is the level of access granted to participants. In the pursuit of decentralization, public blockchains are completely open and allow anyone to participate by verifying or adding data to the blockchain which is also called 'mining'. Whereas in protected block chain, System will check user’s authentication before giving any access permission. In our case we proposed protected blockchain consist of transactions as well as secrete keys of users. In this paper we present a new secure model for document security and searching on cloud. In this model the documents will be stored on cloud in encrypted format using AES algorithm. Before document encryption, the keywords will be extracted from the document and will be stored on cloud server in encrypted format using Caesar algorithm. The keywords format will be reserved by using Caesar algorithm, so that the encrypted keywords will be readable but meaningless. But the secrete key required to encrypt and decrypt document will be stored in blockchain.

II. LITERATURE REVIEW

The searchable encryption technique plays an important role in cloud data storage, where a user can submit a search query to a storage server (e.g., cloud server),[11], [12] and the server is able to respond with the corresponding data without learning anything more about the data content than the search result.[12] The problem of searching on encrypted data is first introduced by Song et al. [1], in which the first scheme for searches on encrypted data was proposed. However, the scheme in [1] requires the server to linearly scan word-by-word of each file, which makes the scheme inefficient. Chang et al. [2] presented a searchable encryption scheme with enhanced security. To improve the efficiency, Goh [3] presented an index-based searchable encryption scheme. The security model of searchable encryption was first defined by Curtmola et al. [4], which requires a secure searchable encryption scheme to leak no more than the search pattern (i.e., whether a search query is repeated) and the access pattern (i.e., pointers to ciphertexts that satisfy search query). Subsequently, many searchable encryption schemes were proposed with different features [5], [6], [7], [8], [9], [10]. These schemes are based on symmetric cryptosystems and are typically applied in the scenario that a user outsources her/his data to the storage server, and later she/he searches the data by keywords.

[1] Here new techniques for remote searching on encrypted data using an untrusted server provided proofs of security for the resulting crypto systems. These techniques have a number of crucial advantages: they are provably secure; they support controlled and hidden search and query isolation; they are simple and fast (More specifically, for a document of length, the encryption and search algorithms only need stream cipher and block cipher operations); and they introduce almost no space and communication overhead. This scheme is also very flexible, and it can easily be extended to support more advanced search queries.

[2]Itstudies the problem how to search on data encrypted by a public-key cryptosystem. In particular, they consider the problem of a user that wants to retrieve e-mails containing a certain keyword from the e-mail server, with the e-mails encrypted by the user using his public key.

[3]The contribution of this paper is in defining a secure index and formulating a security model for indexes known as semantic security against adaptive chosen keyword attack (IND-CKA). The IND-CKA model captures the intuitive notion that the contents of a document are not revealed from its index and the indexes of other documents apart from what an adversary already knows from previous query results and other channels.

[4] The problem of searchable symmetric encryption, which allows a client to store its data on a remote server in such a way that it can search over it in a private manner.

[5]Searchable encryption is an important cryptographic primitive that is well motivated by the popularity of cloud storage services. Any practical SSE scheme, however, should satisfy certain properties such as sublinear (and preferably optimal) search, adaptive security, compactness and the ability to support addition and deletion of files.

[7] The premise of this work is that in order to provide truly practical SSE solutions one needs to accept a certain level of leakage; therefore, the aim is to achieve an acceptable balance between performance and leakage, with formal analysis ensuring upper bounds on such leakage. These solutions strike such a practical balance by offering performance that scales to very large data bases; supporting search in both structured and textual data with general Boolean queries; and confining leakage to access (to encrypted data) patterns and some query-term repetition only, with formal analysis defining and proving the exact boundaries of leakage.

[11] The paper analyzes the requirements of the trustworthiness in cloud storage during their long-term preservation according to the information security theory and subdivides the trustworthiness into the authenticity, integrity, reliability and usability of electronic records in cloud storage. Moreover, the technology of blockchain, proofs of retrievability, the open archival information system model and erasure code are adopted to protect these four security attributes, to guarantee the credibility of the electronic record.

[12] This paper has proposed a blockchain-based security architecture for distributed cloud storage. The proposed architecture has been compared with other two traditional architectures in terms of security and network transmission delay. Based on the simulation assumptions utilized in this paper, the file loss rate of the proposed architecture outperforms other two traditional architectures on average.

III. PROPOSED METHODOLOGY

A. Cloud Documents Encryption

We proposed AES(Advanced Encryption Standards) algorithm with 256 bits key to encrypted uploaded documents on cloud. AES is a more popular and widely adopted symmetric encryption algorithm. AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It consists of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all these computations on bytes rather than bits. Hence, it treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes data are arranged in four columns and four rows for processing as a matrix. The encryption will be held on server side with randomly generated key. After encryption, the documents will be maintained on cloud server only.

B. Secrete key Management

We proposed a partial key storage scheme, in which the system will generate secrete key randomly in alphanumeric format. The randomly generated key will be processed run time at the time of encryption to convert it into 32byte key.Finally, the 32 byte key will be used to perform encryption/decryption. The alphanumeric secrete key required for encryption and decryption will be maintained in blockchain in encrypted format. As we are storing only alphanumeric part of key instead of complete key, the attacker will not be able to guess complete key easily.

C. Keywords Management

Our system will extract text from uploaded document before encryption. The extracted text will be processed to get searching keywords. A typical keyword extraction algorithm contains three main components:

1. Candidate selection:

Here, we extract all possible words, phrases, terms and concepts (depending on the task) that can potentially be keywords.

2. Properties calculation:

For each candidate, we need to calculate properties that indicate that it can be a keyword. For instance, a candidate appearing in the title of a book is a likely keyword.

3. Scoring and selecting keywords:

All candidates can be scored by either combining the properties into a formula, or using a machine learning technique to determine probability of a candidate being a keyword. A score or probability threshold, or a limit on the number of keywords is later used to select the final set of keywords.

- Documents Searching

Document searching will be done over encrypted keywords. The extracted keywords will be encrypted using Caesar algorithm. A Caesar cipher,Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is changed by a letter some fixed number of positions down the alphabet. For instance, with a left shift of 3, D would be replaced by A, E would become B, and so on. After encryption the keywords will be in readable format but will become meaningless.

- Transaction

In our proposed system, along with key storage we also included document purchasing transaction management in blockchain. When any end user purchase particular document, the transaction details will be maintained in blockchain. The transaction details will be accessible to the respective authorized persons.

IV. SYSTEM ARCHITECTURE

In this system, we proposed a generalized document storage cloud server. Any researcher will be able to do registration on this system. The researchers will upload their documents which they want to share with any other user. Our system will store their documents as well as keywords securely on cloud server. If any end user wants to search any document, he will specify search query. Our system will search related documents and display it on screen. If end user wants to access any document he/she has to purchase that particular document by using bit coin transaction. The bit coin transactions will be maintained in blockchain. The transactions will be visible for authorized users only. The architecture diagram is shown below.

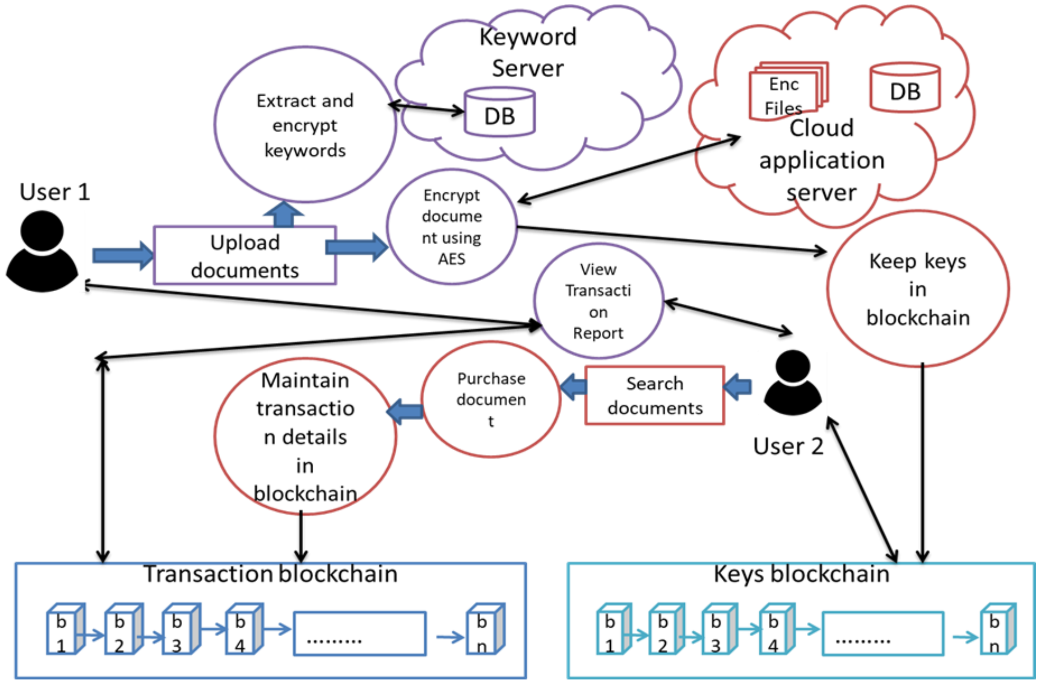

Fig 1 : Working Of Application

V. ALGORITHM AND MATHEMATICAL MODEL

1. Algorithm for encrypting documents on cloud server: Advanced Encryption Algorithm (AES):

Steps:
1) Derive the set of round keys from the cipher text.
2) Initialize the state array with the block data(plain text).
3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of state manipulation.
6) Copy the final state array out as the encrypted data(cipher text).

2. Algorithm for encrypting document keywords:Caesar Algorithm:

Steps:
1) Traverse the given text one character at a time.
2) For each character, transform the given character as per the rule, depending on whether we are encrypting or decrypting the text.
3) Return the new string generated.

Input:
1: A string of lower case letters, called text.
2: An integer between 0 to 25,denoting the required shift.

Mathematical Model:

$$X^0 = P \oplus K$$

$$T := \texttt{SubBytes}(X^i),$$

$$T := \texttt{ShiftRows}(T),$$

$$T := \texttt{MixColumns}(T),$$

$$X^{i+1} := T \oplus K^i.$$

$$C = X^{10} = T^{10} \oplus K^{10}$$

Fig 2 : Function showing the encryption of text using the AES Algorithm. Each round consists of several processing steps, including one that depends on the encryption key . A set of reverse rounds are applied to transform cipher text back into the original plain text.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

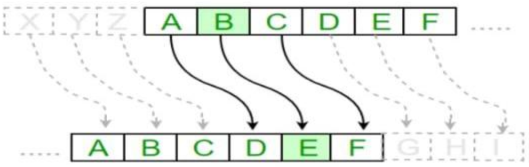

Fig 3 : Function showing the encryption and decryption of keywords using the Caesar Algorithm. After applying this function the result is a numeric value which must then be translated back into a letter.

VI. FLOWCHARTS

1. Working of document encryption on cloud.

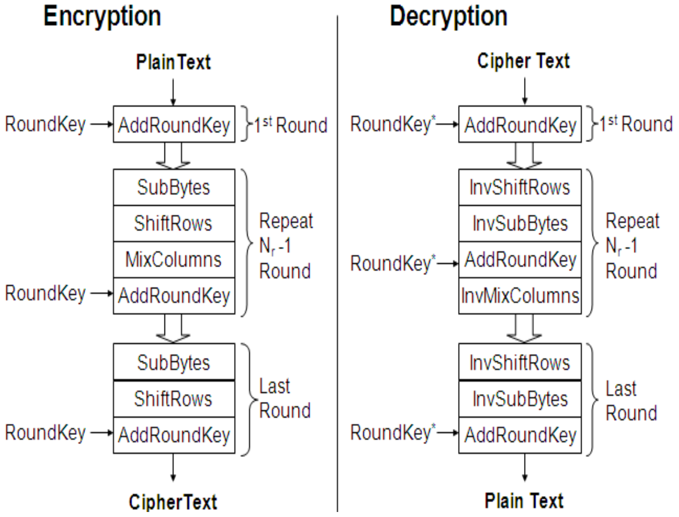

Fig 4. Flowchart for AES Algorithm

2. Working of keyword encryption.

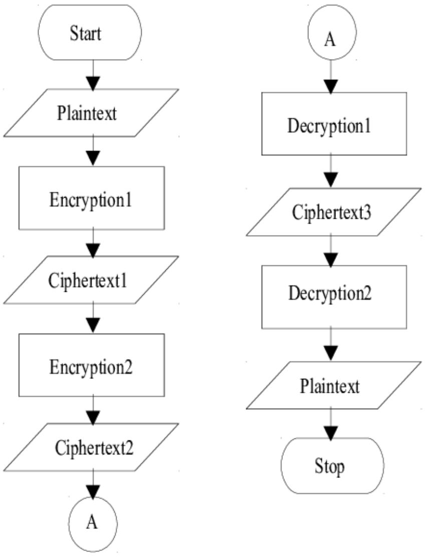

Fig 5. Flowchart for Caesar Algorithm

VII. CONCLUSION

In this paper, secure encryption algorithms with blockchain technology usage for key management has been presented to prevent document leakage from cloud service provider and any other third-party attacker. Also, we presented the use of protected blockchain in transaction management as well as in key management securely. We have proved the security of the proposed system by using blockchain based key storage scheme. Therefore, it can be concluded that the proposed system is very secure and cost efficient for those who wants to store and share their documents with other users securely.

ACKNOWLEDGMENT

We would like to express our profound thanks to Prof.P.B.Lohiya for her guidance and constant supervision as well as for providing necessary information.We would also like to express our gratitude towards

Dr.G.R.Bamnote,Head of Computer Science and Engineering department for their kind co-operation and encouragement .

REFERENCES

[1]. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, 2000, pp. 44–55.

[2]. Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, vol. 5, 2005, pp. 442–455.

[3]. E. Goh, "Secure indexes," Cryptology ePrint Archive, report 2003/216, 2003.

[4]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. of ACM CCS, 2006, pp. 79–88.

[5]. S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of ACM CCS, 2012, pp. 965–976.

[6]. F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in Proc. of ACM CCS, 2014, pp. 310–320.

[7]. D.Cash,S.Jarecki,C.Jutla,H.Krawczyk,M.Ros¸u,andM.Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Proc. of CRYPTO, 2013, pp. 353–373.

[8]. H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[9]. C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Y. Zomaya, "Anefficientprivacy-preservingrankedkeywordsearchmethod," IEEE Trans. Parallel and Distributed Systems, vol. 27, no. 4, pp. 951– 963, 2016.

[10]. H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Trans. Cloud Computing, accepted 2017, to appear, doi. 10.1109/TCC.2017.2769645.

[11]. Zhiliang Deng 1, 2 , Yongjun Ren3, 4 , Yepeng Liu3, 4 , Xiang Yin5 , Zixuan Shen3, 4 and Hye-Jin Kim6, *"Blockchain-Based Trusted Electronic Records Preservation in Cloud Storage"

[12]. Jiaxing Li, Jigang Wu, Long Chen, Block-Secure: Blockchain Based Schemefor Secure P2P Cloud Storage, Information Sciences (2018), doi: 10.1016/j.ins.2018.06.071

Ms. Kaushiki Tapadiya,et.al. "Blockchain Based Secrete Key and Transaction Storage System for Documents Stored on Cloud" *IOSR Journal of Engineering (IOSRJEN),* 10(1), 2020, pp. 13-18