International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTING BLOCKCHAIN ASSISTED PUBLIC KEY ENCRYPTION TECHNIQUE IN CLOUD COMPUTING FOR SECURING DOCUMENTS.

Kuldeep S. Ratawa[1], Dr. Pritish A. Tijare[2]

[1]Post Graduate Student, Sipna College of Engineering & Technology, Maharashtra, India
[2]Professor, Sipna College of Engineering & Technology, Maharashtra, India

---

Abstract - *Cloud store is getting veritably popular now-a-days. It's veritably cost effective to store important documents on cloud. The documents that are stored on cloud server are in translated format, but the keys and keywords also stored on the same server to achieve centralization. However, there's a possibility of document leakage, If we maintain all data on same server. Thus, to ameliorate security of the documents that are stored on cloud server, we proposed blockchain supported public key encryption method. Using this method, the keys of the documents and their keywords will be stored in blockchain rather of cloud server. Along with document security, we concentrate on keywords security. To ameliorate document keywords security, we proposed separate keywords store server.*

Blockchain technology is a core, underpinning technology with promising operation prospects in the banking assiduity. To date, blockchain technology is applicable in all areas and the banking system isn't an exception. Blockchains could revise the underpinning technology of the payment clearing and credit information systems in banks, therefore upgrading and transubstantiating them. Block chain technology should be introduced in the ultramodern banking system, since they give control over crypto currency that will help in neutralizing plutocrat-laundering and backing of terrorism in the country and around the world. In utmost of the literatures, document encryption fashion is described using different algorithms. Cracking documents before store is a good idea, but if translated documents as well as the secrete keys both are maintained on cloud server only, there's a possibility of leakage as the pall service provider is an honest but curious reality. So, it can be a big threat if we maintain documents as well as their keys on cloud. On the other hand, if we apply unbreakable encryption on documents before cloud on cloud also the searching over documents will be critical. Thus, in this paper we concentrate 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, Caesar Algorithm, public key, transaction management.

1. Introduction

Cloud security is a boiling exploration topic in todays world. Multiple literatures are available on document encryption on cloud to give security to the documents stored on cloud. No mistrustfulness encryption plays a vital part in cloud security process, but on the other hand the one who knows translated document as well as key will be suitable to endeavor for decryption. It seems that it isn't enough to cipher cloud documents, rather along with the encryption we've to keep keys out from documents securely. But as we know cloud refers to centralization, if we're considering cloud, it's egregious that complete data is store at one place. Thus, to maintain conceal keys and documents independently, we proposed a new methodology in which documents will be stored on cloud server and secrete keys will be maintain in blockchain.

A blockchain is primarily block chain, is a growing list of records, called blocks that are linked using cryptography. Each block has a hash value of the former block, a timestamp, and transaction data. This technology resists the alteration of data. Blockchain refers to the storage of essential transaction on dissected servers. Blockchain is generally used for bit coin related transaction conduct. There are three different type of block chains are as follow; public, private and protected. The main difference between a private and public blockchain is the ranking of access granted to actors. In the pursuit of decentralization, public blockchains are fully open and allow anyone to share by authenticating or adding data to the blockchain which is also called 'mining'. Whereas in protected block chain, System will check user authentication before giving any access authorization. In our case we proposed protected blockchain correspond of transactions as well as secrete keys of users. In this paper we present a new secure model for document security and searching on server. In this framework the documents will be stored on cloud in encryption form using AES algorithm. Before document encryption, the keywords will be pulled from the document and will be stored on cloud server in encrypted format using Caesar algorithm. The keywords format will be conserved by using Caesar algorithm, so that the encrypted keywords will be readable but will be of no use. But the secrete key needed to cipher and decipher document will be stored in blockchain. Cloud

computing is high on- demand obtainability of computer system resources, especially data storehouse and calculating power, without direct active operation by the user. Large clouds, predominant now a days, frequently have functions distributed over multiple positions from central servers. If the connection to the user is considerably close, it may be delegating an edge server. The accessibility of high-capacity networks, low-end computers and storage devices as well as the wide adoption of hardware virtualization, service-oriented framework and autonomic and utility computing has led to growth in cloud computing. A blockchain, is a growing list of dissected records, called blocks, that are linked with each other using cryptography. Every block has a cryptographic hash of the previous block, timestamp, and transaction data (generally represented as a Merkle tree). It is an user ended framework which can keep the minute details in the dissected form of transaction between the two users ".

Generally, framework include store-and-forward systems, such as cloud-based email systems, where more than one user (called senders) are willing to send data containing a small number of keywords to one user (called receiver). tiple users (called senders) are willing to send data containing a small number of keywords to one user (called receiver). Senders are able to allocate the data as well as keywords to the storage server, and the receiver can recover target data from the storage server through searching by keywords. This can reduce load of senders and the receiver from heavy local storage costs, and allows the receiver to access the required data on other devices (e.g., smartphones) at a later point in time. On the other hand, as the documents and keywords used to maintain on third party cloud; the security will be totally dependent on cloud service provider. Cloud storage is becoming very popular now-a-days. It is very cost efficient to store important documents on cloud. The documents that are stored on cloud server are in encrypted format, but the keys and keywords also stored on the same server to achieve centralization. If we maintain all data on same server, there is a possibility of document leakage. Therefore, to improve security of the documents that are stored on cloud server, we proposed blockchain assisted public key encryption technique. Blockchains are generally built to augment the score of nascent blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the chances of an entry becoming succeed decreases exponentially.

2. Literature Review

The concept of block chain was proposed by an individual name Satoshi Nakamoto in 2008 as he was anarchist and did not believe of fiat money. Nakamoto efficiently design an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a hard parameter equalize rate with which blocks are augmented to the chain. The framework was applied the following year by Nakamoto as a main component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network. In August 2014, the bitcoin blockchain file size, containing data of all transactions between the user that have occurred on the network, reached 20 GB (gigabytes). In January 2014, the size had grown to almost 40 GB, and from January 2016 to January 2018, the bitcoin blockchain grew from 50 GB to 100 GB in size. The ledger size has been increased by 200 GiB by early 2020. The words block

and chain were applied individually in Satoshi Nakamoto's original paper, but were latter popularized as one word, blockchain, by 2016. According to researcher, an application of the diffusion of innovations theory suggests that blockchains achieve a 14.5% adoption rate within financial transaction in 2017, therefore reaching the first adopter's phase. Industry trade groups joined to form the worldwide Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce. In May 2018, Gartner found that just one of CIOs indicated any quite blockchain adoption within their organizations, and only 8% of CIOs were within the short-term "planning or [looking at] active experimentation with blockchain".

Cloud computing was popularized with Amazon.com releasing its Elastic Compute Cloud product in 2006.In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) method with comparable level of methods, but at a efficient cost. By switching traffic as they saw fit balance server use, they might use overall network bandwidth more effectively. They started to use the cloud symbol to show the demarcation point between what the provider was liable for and what users were liable for. Cloud computing increase its boundary to ensure all servers as well as the network infrastructure. As computers became more dissected, researchers and technologists explored ways to form large-scale computing power available to more users through time-sharing. The research work with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users.

In July 2011, Rackspace Hosting and NASA jointly launched an open-source cloud-software initiative referred to as OpenStack. The OpenStack project intended to assist organizations offering cloud-computing services running on standard hardware. The early code came from NASA's Nebula platform also as from Rackspace's Cloud Files platform. As an open-source offering and along with other open-source solutions such as Cloud Stack, Ganeti and Open Nebula, it has attracted attention by several key communities. Several studies aim at comparing these open-source offerings supported a group of criteria. Here

new technique for remote searching on encrypted data using an untrusted server provided verification of security for the resulting crypto systems. These techniques have variety of crucial advantages: they're provably secure; they support controlled and hidden search and query isolation; they're simple and fast; and they introduce almost no space and communication overhead. This method is also very tensile, and it can efficiently be extended to support more advanced search queries. It studies the problem how to search on data encrypted by a public-key cryptosystem. In particular, they consider the matter of a user that desires to retrieve e-mails containing a particular keyword from the e-mail server, with the e-mails encrypted by the user using his public key. The benefaction of this research is in defining a secure index and computing a security infrastructural for indexes referred to as semantic security against adaptive chosen keyword attack (IND-CKA). The IND-CKA method captures the instinctive notion that the contents of a document aren't revealed from its index and therefore the indexes of other documents aside from what a problem already knows from previous query results and other channels.

The problem of searchable symmetric encryption, which allows a client to store its data on a foreign server in such how that it can search over it during a private manner.

Searchable encryption is a crucial cryptographic primitive that's well motivated by the recognition of cloud storage services. Any practical SSE scheme, however, should satisfy certain properties like sublinear (and preferably optimal) search, adaptive security, compactness and therefore the ability to support addition and deletion of files.

[7] The premise of this work is that so as to provide truly practical SSE solutions one must accept a particular level of data breach; therefore, the aim is to realize a suitable balance between performance and leakage, with formal analysis ensuring upper bounds on such leakage. These methods strike such a practical equilibrium by offering performance that scales to very large data bases; supporting search in both structured and textual data with general Boolean queries; and confining data breach to access (to encrypted data) design and a few query-term repetition only, with formal analysis characterize and providing the precise limitation of data breach.

[11] The paper analyzes the wants of the trustworthiness in cloud storage during their long-term preservation consistent with the knowledge security theory and subdivides the trustworthiness into the authenticity, integrity, reliability and usefulness of electronic records in cloud storage. Moreover, the technology of blockchain, proofs of retrievability, the open archival data system model and erasure code are adopted to guard these four security attributes, to ensure the credibility of the electronic record.

[12] This research has proposed a blockchain-assisted security framework for distributed cloud storage. The proposed framework has been contrasting with other two traditional framework in terms of security and network transmission lag. supported the simulation assumptions utilized during this paper, the file loss rate of the proposed framework master other two conventional architectures on the average.

3. Problem Analysis

In existing cloud storage system, documents and keywords along with their keys used to maintain on single cloud server. There is a possibility of document/ keywords leakage, therefore to improve security of the system we proposed blockchain assisted key encryption technique

4. Propose Work

A. Cloud Documents Encryption

We proposed AES (Advanced Encryption Standards) algorithm with 256 bits key to encrypted transmit data on cloud. AES is a more accessible and widely adopted symmetric encryption algorithm. AES is a repetition instead of Feistel code. It is based on substitution–permutation network". It comprises of a series of linked method, some of which involve replacing inputs by specific outputs (substitutions) and others method shuffling bits around (permutations). Interestingly, AES performs of this calculation on bytes rather of bits. Hence, it takes the 128 bits of a plaintext block as 16 bytes. These 16 bytes data are layout in four columns and 4 rows for computing as a matrix. The encryption goes to be persisted server side with randomly generated key. After encryption, the data are going to be carried on cloud server only.

B. Secrete Key Management

We proposed a partial key storage scheme, during which the system will generate secrete key randomly in alphanumeric format. The randomly generated key are going to be processed run time at the time of encryption to convert it into 32byte key. Eventually, the 32-byte key are going to be used to perform encryption/decryption. The alphanumeric secrete key required for encryption and decryption are going to be maintained in blockchain in encrypted format. As we are storing only alphanumeric a part of key rather than complete key, the intruder won't be able to guess complete key easily.

C. Keywords Management

The system extracts the info from document and after extracting data it'll be encrypted. The extracted text goes to be processed to impulse searching keywords. a particular keyword extraction algorithm generally

contains three main elements:

1. Candidate selection:
Here, we abstract all feasible words, phrases, sentences and ideas (depending on the assignment) which will potentially be keywords.

2. Properties computation:
For each candidate, we'd like to compute properties that shows that it is often a keyword. as an example, a candidate appearing within the title of a book may be a likely keyword.

3. Scoring and opting keywords:
All candidates are often seamed by either combining the properties into a formula, or by using the tactic of a machine learning technique to see 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 last word set of keywords.

• Documents Searching
Document searching are going to be done over encrypted keywords. The extracted keywords from the encrypted keyword are getting to be encrypted using Caesar algorithm. A Caesar cipher, Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one among the only and most extensively known encryption techniques. it's a kind of substitution cipher during which each letter within the plaintext is modified by a letter some fixed number of positions down the alphabet. it's sort of technique during which, with a left shift of three, D would be displace by A, E would become B, and so on. After encryption the keywords are getting to be in readable format but will become pointless.

• Transaction
In our proposed framework, alongside key storage we also involve document purchasing transaction management in blockchain. When any user subscribes particular document, the transaction details are going to be conserve in blockchain. The transaction details are going to be handy to the respective authorized user.

5. System Design

In this architecture, we put forward a generalized document storage cloud server. Any researcher or user will be able to do registration on this framework. The user will upload their documents or research related work which they want to share with any other user or client. Our framework will store their documents/data 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 affiliated documents and display it onscreen. If end user wants to access any document, he/she has to subscribe that particular document by using bit coin transaction or any such prescribe by admin. The bit coin transactions are going to be maintained in blockchain. The transactions will be visible for the users who have been given permission only. The architecture diagram is shown below.

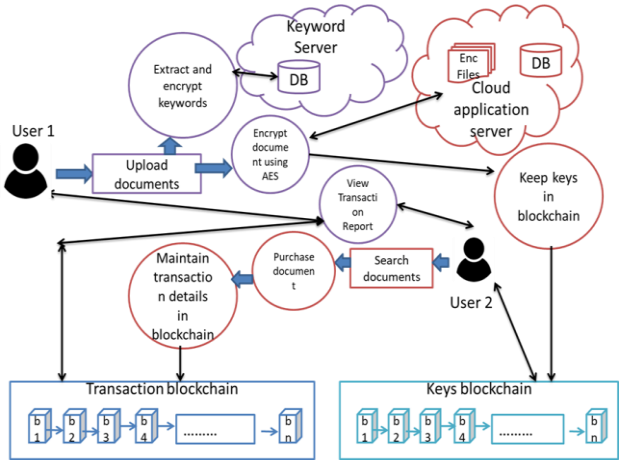

Fig: Working of Application

ALGORITHM AND MATHEMATICAL MODEL

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

Steps:

1) Obtain the set of round keys from the ciphertext.
2) Modify the state array with the block data(plaintext).
3) Augment the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Carry out the tenth and final round of state manipulation.
6) Replicate the final state array out as the encrypted data(ciphertext).

2. Algorithm for encrypting document keywords: Caesar Algorithm:

Steps:

1) Traverse the whole text, one character at a time.
2) For each character, alter the given character as per the rule, depending on whether we are encrypting or decrypting the text.

6. Implementation

In this project we implement a new technique in which the documents will be maintained on cloud server and the keywords will be maintain on key server separately. To distribute keys, we use blockchain technology. Along with keys we will maintain transaction in blockchain. This project is a combination of centralized as well as

distributed storage. To encrypt document, we proposed AES algorithm. AES algorithm is a symmetric algorithm and encrypt document using secrete key.

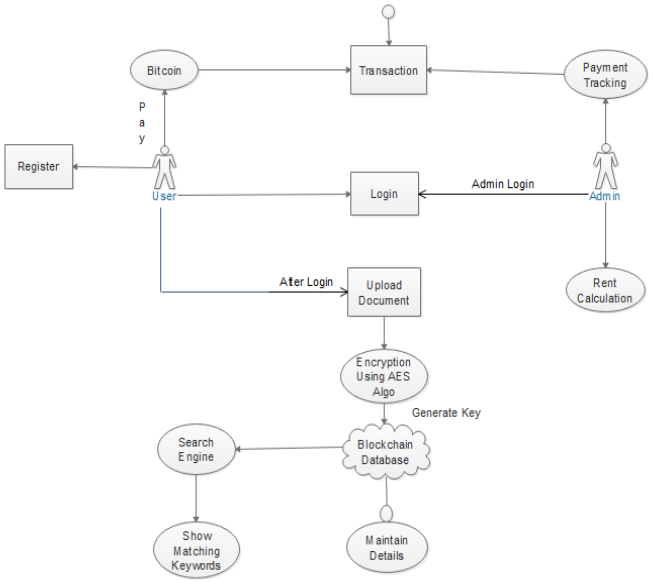

Fig: Flow chart

The above diagram illustrates the info flow chart , It consists different processes, actions, users, etc. The new users can perform multiple functions like Register as new user, login, look for the documents, can buy document by performing bitcoin transaction, upload their own documents, images, etc. Admin have different bunch of functions to perform like login, maintain service charges per users, payment tracking, rent calculations etc. Once the user uploads a document it gets encrypted. User can share the encrypted document freed from cost or with subscription.

7. Result Analysis

It is observed that the user who want to send or sell the pdf or the research paper work can register. Then he can login by using the credentials which he receives on the e-mail. After doing login he can select and upload the pdf or the research related work which can be within the encrypted form and therefore the user who has allowed permission or paid the specified subscription can access the pdf. it'll prevent any 3rd party user to getting access thereto. In today's world, one among the most important problems in digital advertising is challenges like domain fraud, bot traffic, lack of transparency and long payment models. Blockchain can provide solutions to those problems because the technology will only allow the proper companies to succeed

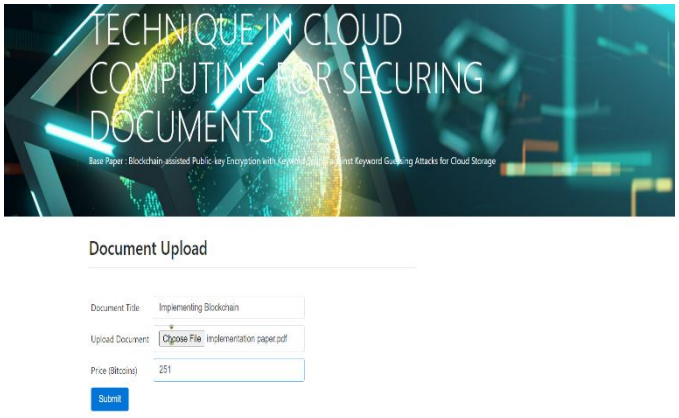

Fig: Document uploaded

Fig: Permission allotted

8. Conclusion

In this Project, secure encryption algorithms with blockchain technology usage for key management has been presented to stop document leakage from cloud service provider and the other third-party attacker. Also, we demonstrated the utilization of protected blockchain in transaction management also as well as in key management securely. We've have demonstrated the safety of the proposed system by using blockchain based key storage scheme. Therefore, it can be concluded that the proposed system is extremely secure and price efficient for those that wants to store and share their documents with other users securely

9. 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, "Anefficient privacy- preserving ranked keyword search method," 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 Scheme for Secure P2P Cloud Storage,.