REVIEW ON 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 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. Using this technique, the keys of the documents and their keywords will be stored in blockchain instead of cloud server. Along with document security, we focus on keywords security. To improve document keywords security, we proposed separate keywords storage server.*

Blockchain technology is a main technology with promising result and application prospects within the core banking system. Up to date, blockchain technology is useful in all fields and the banking system is not an exception. Blockchains could revolutionize the underlying technology of the payment clearing and credit information systems in banks, thus upgrading and reworking them. Block chain technology should be introduced within the modern banking industry, since they supply control over crypto currency which will help in counteracting money-laundering and financing of terrorism in the country and around the world.

Keywords— Blockchain, Benefits from Blockchain, Decentralized consensus, Features of Blockchain Security, Aspects of Blockchain, Smart contracts.

1. Introduction

Cloud computing is the on- demand vacuity of computer system resources, especially data storage and calculating power, without direct active operation by the user. Large shadows, predominant moment, frequently have functions distributed over multiple locales from central servers. However, it going to be designated a base server, If the connection to the user is comparatively close. The vacuity of high- capacity networks, low- cost computers and storage bias also because the wide relinquishment of tackle virtualization, service- acquainted architecture and automatization and use of computing has resulted to growth in cloud computing. A blockchain, consist of growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, timestamp, and transaction data (generally represented as a Merkle tree).Its an distributed leger which keeps the track of all the transaction. Typical applications include store-and-forward systems, such as cloud-based email systems, where multiple users (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 ready to outsource the info also as keywords to the storage server, and therefore the receiver can retrieve target data from the storage server through searching by keywords. This can free senders and therefore the receiver from heavy local storage costs, and allows the receiver to access the target 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 typically built to feature the score of latest blocks onto old blocks and are given incentives to increase with new blocks instead of overwrite old blocks. Therefore, the chance of an entry becoming override reduce exponentially.

2. Literature Review

The first blockchain was visualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improvised the architecture in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a different parameter to stabilize rate with which blocks are added to the chain. The design was enforced the ensuing time by Nakamoto as a core element

of the cryptocurrency bitcoin, where it serves as the public tally for all deals on the network. In August 2014, the bitcoin blockchain train size, containing records of all deals that have passed on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to nearly 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The tally size had exceeded 200 Kit by early 2020.The word block and chain where use by Satoshi Nakamoto research individually but latter on they where use combinedly, blockchain, by 2016. According to Accenture, an operation of the prolixity of inventions proposition suggests that blockchains attained a13.5 relinquishment rate within fiscal services in 2016, thus reaching the early adopter's phase. Assiduity trade groups joined to produce the Global Blockchain Forum in 2016, an action of the Chamber of Digital Commerce. In May 2018, Bartner plant that only 1 of CIOs showed any kind of blockchain relinquishment within their associations, and only 8 of CIOs were in the short- term "designing or (looking at) active demo with blockchain".

Cloud computing was vulgarized withAmazon.com releasing its Elastic Compute Cloud product in 2006. In the 1990s, telecommunications companies, who preliminarily offered primarily devoted point-to- point data circuits, began offering virtual private network (VPN) services with similar quality of service, but at a lower cost. By switching business as they saw fit to balance server use, they could use overall network bandwidth more effectively. They began to use the pall symbol to denote the discrimination point between what the provider was responsible for and what user were responsible for. cloud computing extended this boundary to cover all waiters as well as the network structure. As computers came more diffused, scientists and technologists explored ways to make large-scale computing power available to further druggies through time-sharing. They experimented with algorithms to optimize the structure, platform, and operations to prioritize CPUs and increase effectiveness for end druggies.

In July 2010, Rackspace Hosting and NASA concertedly launched an open- source pall-software action known as OpenStack. The OpenStack design intended to help associations offering pall-computing services running on standard tackle. The early law came from NASA's Nebula platform as well as from Rackspace's Cloud Lines platform. As an open- source immolation and along with other open- source results similar as Cloud Stack, Ganeti and Open Nebula, it has attracted attention by several crucial communities. Several studies aim at comparing these open-source immolations grounded on a set of criteria. Then new ways for remote searching on translated data using an untrusted garçon handed attestations of security for the performing crypto systems. These ways have a number of pivotal advantages they're provably secure; they support controlled and hidden hunt and query insulation; they're simple and fast (More specifically, for a document of length, the encryption and hunt algorithms only need sluice cipher and block cipher operations); and

they introduce nearly no space and communication outflow. This method is also veritably flexible, and it can efficiently be extended to support more advanced search queries.

It studies the drawback how to search on data encrypted by a public-crucial cryptosystem. In particular, they consider the matter of a user that desires to retrieve e-mails consisting a particular keyword from thee-mail server, with thee-mails encrypted by the user using his public key. The benefaction of this paper is in defining a secure indicator and formulating a security model for indexes known as semantic security against adaptive chosen keyword attack (IND-CKA). The IND-CKA model catches the instinctual notion that the datas of a document are not revealed from its index and thus the indexes of other documents apart from what an adversary antecedently knows from former query results and other channels.

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

Searchable encryption is an important cryptographic primitive that's well motivated by the high demand of cloud storage services. Any practical SSE scheme, still, should satisfy certain properties like sublinear (and preferably optimal) hunt, adaptive security, conciseness and thus the capability to support addition and omission of lines.

(7) The premise of this work is that in order

to give truly practical SSE results one must accept a particular degree of leakage; thus, the idea is to realize a suitable balance between performance and leakage, with formal analysis assuring upper bounds on such leakage. These results strike such a practical balance by offering performance that scales to veritably large data bases; supporting search in both structured and textual data with general Boolean queries; and confining leakage to penetrate (to encrypted data) patterns and a limited query- term iteration only, with formal analysis defining and proving the precise boundaries of leakage.

(11) The paper provides the conditions of the responsibility in cloud storage during their long- term preservation according to the data security proposition and subdivides the responsibility into the authenticity, integrity, trustability and utility of electronic records in cloud storage. Also, the technology of blockchain,

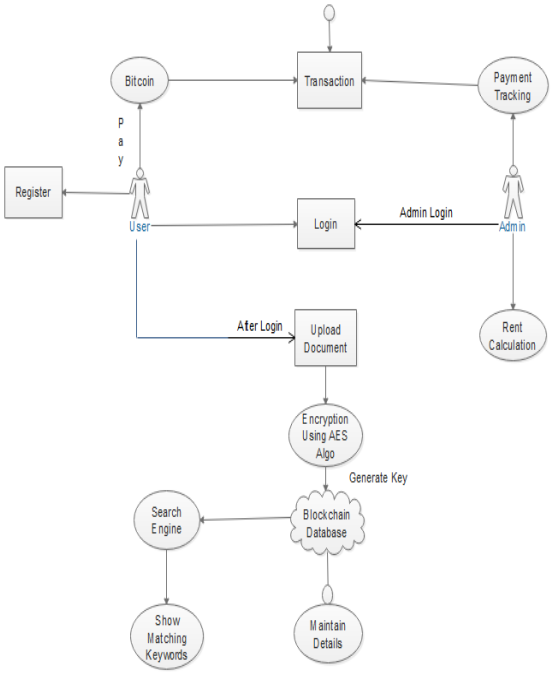
validations of retrievability, the open archival information system model and erasure code are taking up to safeguard these four security attributes, to guarantee the credibility of the electronic record.

(12) This paper has proposed a blockchain- assisted security framework for distributed cloud storage. The proposed armature has been compared with other two traditional frameworks in terms of security and network transmission slow down. Derived on the simulation hypotheticals use during this paper, the file loss rate of the suggested framework performs well than other two traditional frameworks on the par**.**

3. PROPOSED WORK

In this project we proposed a new technique in which the documents will be maintained on cloud server and the keywords

will be maintain on crucial garçon independently. To distribute keys, we use blockchain technology. Along with keys we will maintain sale in blockchain. This design is a combination of consolidated as well as distributed storehouse. To cipher document, we proposed AES algorithm. AES algorithm is a symmetric algorithm and cipher document using cache key.



Data Flow Diagram

1. The above illustration illustrates the data inflow illustration, It contain different method, conduct, user, etc. The new users can conduct multiple functions like Register as new client, login, hunt for the documents, can purchase document by performing bitcoin sale, upload their own documents, images, etc. Admin have different type of functions to perform like login, maintain service charges per user, payment shadowing, rent computations etc. Once the stoner uploads an document it get translated performs some internal action Algorithm for encrypting documents on cloud server: Advanced Encryption Algorithm (AES):

Steps:

1) Obtain the set of round keys from the ciphertext.

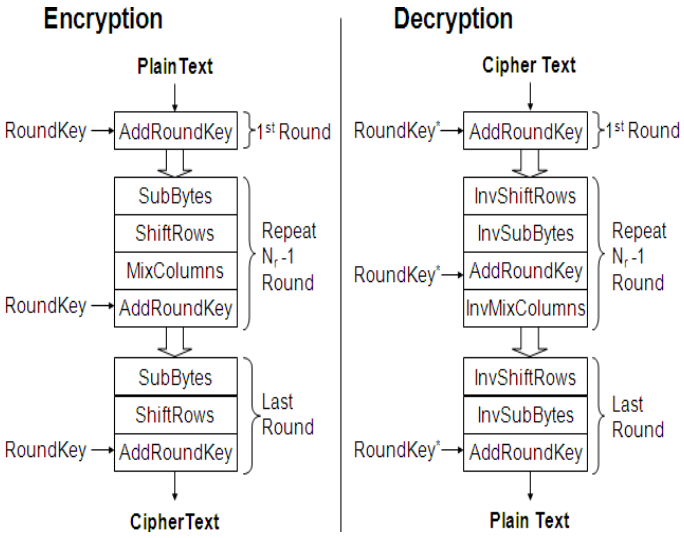
2) Initiate the state array with the block data(plaintext).

3) Sum the initial round key to the starting state array.

4) Execute nine rounds of state manipulation.

5) Execute the tenth and final round of state manipulation.

6) Imprint the final state array out as the encrypted data(ciphertext).



AES algorithm Steps

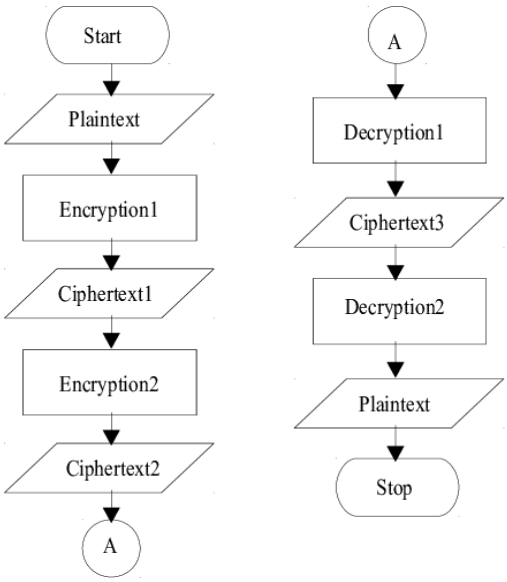
2. Algorithm for encryption of the document keywords: Caesar Algorithm:

Steps:

1) Traverse the whole given text one character at a time.

2) For each cross character, transform the given character as per the rule and regulation, depending on whether that we are encrypting or decrypting the text.

3) Return the new string generated.



Flowchart for AES Algorithm

Databases

MySQL is free and open- source software under the terms of the GNU General Public License, and is also available under a variety of particularly licenses. MySQL was held and patronized by the Swedish company MySQL AB, which was bought by Sun Microsystems now Oracle Corporation.2010, when Oracle bought Sun, Widenius diverged the open-source MySQL design to produce MariaDB. MySQL can also be run on cloud computing platforms such as Microsoft Azure, Amazon EC2, Oracle Cloud framework. In this application, cloud users can upload a machine image of their own with MySQL installed, or use a ready-made machine image with an optimized installation of MySQL on it, similar as the one provided by Amazon EC2.

4. Conclusion

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

5. 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,.