Design of Secured Cloud Architecture Using Blockchain Technology

Mr. Amarnath J L[1], Dr. Pritam G Shah[2], Dr. Sarika Malhotra[3], Dr. Sharmila[4]
[1]Research Scholar at VTU Belagavi [2]Chief Editor at Australian Journal of Wireless Technologies, Mobility and Security, University of Canberra, [3]Associate Professor,
JSPMs Imperial College of Engineering and Research, Pune [4]Lecturer Electronics, Gov. Girls Polytechnic, Bareilly, U.P, India

***Abstract*—Cloud computing is one of the significant technologies that gained more popularity in less time as it provides low cost solutions and reduces the complexity of applications, flexibility and scalability. But, still it suffers from the specific security challenges concerned to loss of control, trust and multi-tenancy in the cloud model. This paper presents a novel secured cloud architecture using blockchain technology. This architecture also uses the ciphertext-policy attribute-based encryption (CP-ABE) for encryption process. This architecture is the decentralized, i.e. there is no trusted third party involvement. It uses blockchain technology for storing the ciphertext data through Smart Contracts (SCs). The data owners can set the valid access periods for the users for the decryption of the ciphertext data during that interval. The functional trace can be achieved by creating and invocating the each SC in blockchain. Since this design is based on the blockchain technology, it is more efficient and secure than all other algorithms.**

***Index Terms*—Blockchain, Cloud, Cloud Computing, Encryption, Decryption and Cloud Security.**

I. Introduction

Cloud computing [1] is one of the biggest technology revolution around us. It is changing the way consumers consume services, changing the ways organizations develop and run applications and completely reshaping old business models in multiple industries. It is providing a growing amount of opportunities for small and big businesses to expand into new markets innovate more quickly and create new value. Applications and data are sitting somewhere in the cloud managed and operated by someone else and the Applications and data are sitting somewhere in the cloud managed and operated by someone else and the worldwide. This revolution must be supported by people that can understand the underlying technology, the best options in the market, the business value and evaluate the opportunities and also the risks. Cloud computing is touching almost any corner in our life. It is transforming the IT world and the impact wave is going in spreading around. Anyone in the high-tech industry should learn cloud computing and add cloud skills. Cloud computing is a quite comprehensive subject with multiple layers and it makes sense to divide it into more small manageable components.

Cloud Computing [2, 3] is becoming a more mature and accepted solution for replacing or even enhancing traditional. It was started as emerging new technologies and now it is an established internet based solution that is gaining widespread acceptance. More and more business companies and organization are moving in that direction. As a result, the market movement is already influencing multiple industries and it is really considered a major disruptive force in the market. It is completely changing the IT industry, transforming the basic business models that were used for so many years. But more important than that is the horsepower of public cloud services are now available to everyone, to every company that is smart enough to utilize it for their business advantage. Cloud Computing is not really just about saving money. It is perceived by more and more companies as a catalyst for innovation. It is shown in fig. 1.

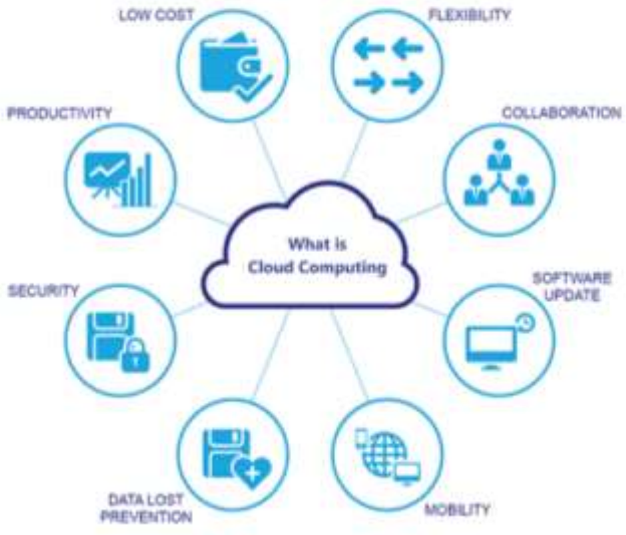

Fig. 1: Block diagram of Cloud Computing

We already show that digital businesses require speed and agility that cloud computing can provide through the use of cloud services, because it enables global reach of services and information through an elastic computing environment that is easy to use. This is one of the reason why it is important to invest in cloud skills. The market demands for cloud skills is increasing in multiple directions, from developing new cloud applications, migrating existing applications to the cloud, promoting and selling cloud solution, utilizing newly advanced services offered by cloud providers and so on. More than that, innovation across multiple industries is rapidly shifting to the cloud and we will see more and more vendors, companies that provide products and services, they will provide their solution mainly in the cloud, meaning their product and services will be available mainly as a cloud services. Now the cloud is also become a catalyst for small business growth because it allows them to innovate and more easily penetrate existing well-established markets and even create completely new markets, new business models. New types of business models are entering the market, taking, for example, the whole e-learning digital banks, all of them are heavily based on technologies, digital data, analytics, network connectivity and so on. The adoption data rate is growing, big companies started to embrace it as a strategic decision, to focus on the core business and utilize the power of cloud services. Multiple cloud service providers are in growing competition, who grabs more market share in this growing cake. Cloud computing is really becoming the mainstream, and everything is online and connected. It's characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Each one of them is an important building block for almost any cloud service and cloud solution being used today.

Cloud computing is on demand computing resources delivered to the user over the Internet. The user needs access to some sort of computing. Maybe it's an application the user needs to run. Maybe it's just a server that needs to be started for your company no matter what it is. The cloud can provide those on demand resources and they're delivered to the user in most cases. Basically it's the computing that the user needs but it's done by someone else and it's done somewhere else. Virtualization cloud computing is an approach to computing that leverages the efficient cooling of an on demand self manage virtual infrastructure. But in general cloud computing is the accessing of a large pool of resources to gain access to the applications that the user needs and the user can manage those applications and those resources.

A cloud is elastic meaning it can scale up or down. The cloud is also metered meaning the user only pay for what the user use so there's no long term contracts in most cases and in most cases the user just pay by the minute or by the computing resource whatever it is the user is able to pay in very small increments just like the electric utility or the water service. A cloud of self-service, meaning there is no or there is reduced need for I.T. experts.

II. Prior-knowledge

i. Access Tree

It is a tree structure [1, 4, 5] used to define an access policy that describes an authorized access set as shown in the fig. 2. It consists of leaf nodes and non-leaf nodes. The leaf node consists of attributes whereas the non-leaf nodes consist of threshold values.

Let n_X and t_X denote the no. of child nodes and threshold value of a particular node *x* such that $1 \leq t_X \leq n_X$. If $t_X = n_X$ then that node denotes the "AND" gate logic. If $t_X = 1$ then it denotes "OR" gate logic. The terms *parent*(*x*), *att(x)* and *index(x)* represent the parent node of *x*, attribute set and no. of child nodes of *x*.

Suppose that there are 4 attributes in the access tree and they are assumed as {graduate, professor, computer science, network security}. Only two types of people that who satisfies the access tree are shown in the figure 2. So, it consists of 2 attribute sets, in which the first one is {computer science, network security, professor} that represents the professors in the Institute of Network Security at the School of Computer Science and the second one is {computer science, network security, graduate} that represents the graduates in the School of Network Security at the School of Computer Science.

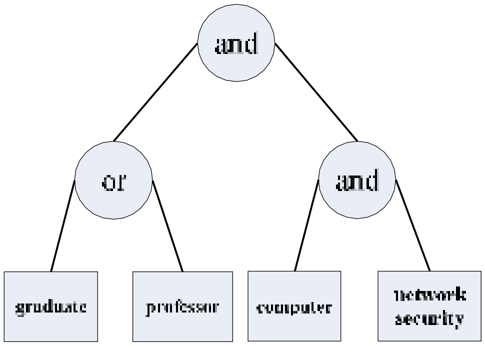

Fig. 2: Access tree structure

ii. Blockchain Technology [6]

Blockchain is considered as the biggest revolutionary technology because it can reinvent the way we work and live. It is presented in different perspectives and applied to different contexts that are like monetary scenarios, security, etc. We can discuss about it in both analytical and practical methods to focus on its most relevant research trends, also we can investigate the methods to adopt the blockchain security for cloud computing. It is a distributed architecture that makes use of cryptographic signed transactions. This technology works in block-wise manner and these blocks are linked with cryptographic systems.

III. Literature Survey

In the paper [7], the authors H. Xu, J. Cao, J. Zhang, L. Gong and Z. Gu, have analyzed the security issues of cloud computing environment. They also briefed about the blockchain technology and its applications in cloud computing. They have summarized the blockchain technology for the solution of the cloud data security threats. They have proposed new cloud forensic storage architecture with blockchains that protects the cloud data.

CloudBC - to protect the cloud data, a secure management access system was implemented using the blockchain technology [8] by S. Ramamoorthy and B. Baranidharan. It is a hybrid architecture that combines the blockchain technology and cloud computing to provide the data security. Also, it can restrict from malicious access of data and its modifications. Here, blockchain helps the users to trace back such activities.

In the paper [9], G. Sharma, L. Ahuja and D. P. Goyal have presented the design of secure infrastructure for cloud computing using blockchain technology. Different platforms have not been yet exposed for the radical cloud conditions of data integrity. It helps in exploiting the various platforms in extreme situations using Blockchains and proposes a more stable and secured cloud infrastructure. In paper [10], ChainFS, a middleware system was proposed by Y. Tang et al., to secure the cloud storage using the blockchain technology. They have designed an algorithm to oppose the forking attacks. It provides a file-system interface to the users. Here, the key distributions and file logging operations are performed using blockchains The paper [11], by N. Tapas, G. Merlino, F. Longo and A. Puliafito describes about the malicious interests at the provider side can alter, hide the data or perform denied access operations. It can be solved by identifying and designing a new protocol that produces a trail of all interactions among the users and providers. It can be performed by introducing the blockchain-based solution.

The authors W. Zheng, Z. Zheng, X. Chen, K. Dai, et. al., have developed a BaaS platform [12] to provide the blockchain techniques for the cloud services like network deployment and system monitoring, smart contracts and testing. It can ease the developers for the applications of blockchain to their business scenarios. Blockchain technology in cloud computing environment increases the security and decreases the vulnerabilities [13]. In this technology, data hacking is more difficult as it is stored in the different blocks and they are stored in different locations of the hard drive. A survey has been carried out on the security issues related to cloud computing environment and blockchain technology [14]. The authors S. Prianga, R. Sagana and E. Sharon have presented a PoW–based blockchain architecture to resolve problems of FaaS. As it's decentralized and peer-to-peer nature to accomplish various requirements of cloud.

Cloud computing with blockchain framework by N. Sanghi, R. Bhatnagar, G. Kaur and V. Jain [15] was presented to analyze the different problems in cloud services. A detailed survey has been carried out mentioning the risks and difficulties associated with cloud computing. Also explained about how the blockchains with cloud computing environments preserve the user data integrity.

CP-ABE scheme was proposed by Zhang P, Chen Z, Liang K, et al. that supports the user revocability and attributes update [16]. The user revocation was defined with identification settings to avoid conflicts with the attribute-based design. The security analysis has been implemented using the decisional Bilinear Diffie-Hellman technique.

IV. System Architecture

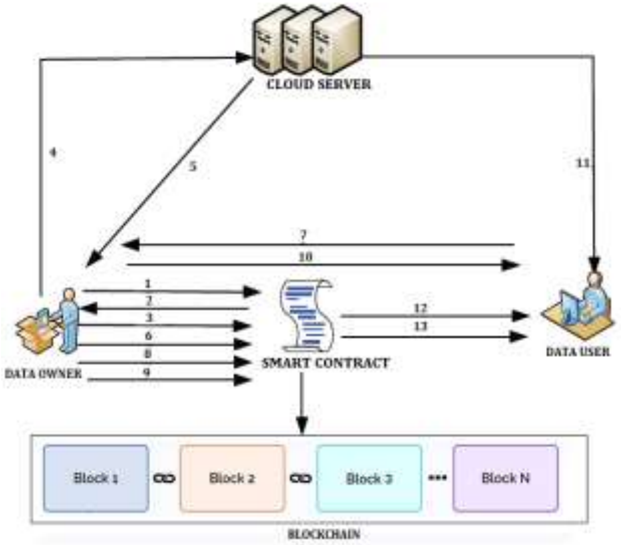

Fig. 3: Secured Cloud Architecture Using Blockchain Technology

The proposed system design of secured cloud architecture using blockchain technology is shown in fig. 3. It mainly consists of four modules i.e. the cloud server, blockchain, data owners and data users. It uses smart contract for the purpose of storing the encrypted file information. Here, both the users and the owners can utilize the blockchain smart contracts that stores and retrieves ciphertext data and runs encryption and decryption algorithms. All the contracts and their call records are stored in the blockchains so that the data will not be tampered and cannot be repudiated.

Here, the cloud server stores the encrypted files uploaded by the data owner. The blockchain can deploy smart contract (SC) and provides interface to store and retrieve the data. The important tasks of a data owner are to create and deploy the SC and upload the encrypted files. Also, it defines the access control policies, assigns the attributes and appends the valid access interval to each user. The responsibilities of a data user are to access the encrypted files that are stored in the server. If its attributes satisfy the access structure embedded in a given ciphertext then it decrypts the received ciphertext to obtain the content key for the decryption operation.

The detailed steps of the proposed architecture are explained as given below:

Step 1: The smart contract named *StorageSC* is deployed by data owner in the blockchain

Step 2: After the successful deployment, the contract address will be returned.

Step 3: Data owner will store the file *ID*, hash H_{ID} in the SC.

Step 4: Data owner packages the contract address contractAddress, file *ID*, and encrypted file E_{Ckey} *(M)* to upload it on the server.

Step 5: Next data owner will record the file path returned by cloud server.

Step 6: Now, the data owner will store the ciphertext of the encrypted document key in the blockchain.

Step 7: Data user will send an access request to data owner.

Step 8: Data owner will add an effective period to data user to store it in the SC.

Step 9: Data owner will encrypt the secret key of data user to store it in the SC.

Step 10: Data owner will send the contract address and user information using the secure channel.

Step 11: Data user will download the encrypted file from the cloud server.

Step 12: Data user will obtain the effective period from the SC.

Step 13: Data user will obtain his secret key ciphertext from the SC.

The following algorithms have been used in this implementation:

Setup-Algorithm: The data owner executes this algorithm. It consists of *k*- security parameters and the universal set *U* of attributes as the inputs. The public key P_K and the master key M_K are obtained by executing this algorithm also the smart contract named *StorageSC* is deployed immediately in the blockchain. AES symmetric encryption algorithm is used for the encryption of file then it is uploaded on the server and records it as E_{Ckey} *(M)* where C_{key} is the encryption key.

Encryption Algorithm: It is given by the inputs i.e. public key P_K, access structure *T* and symmetric encryption key *ck* and generates ciphertext *C* as an output. The ciphertext *C* is stored by data owner in the SC.

Key Generation Algorithm: It is executed by the data owner. The data user sends an access request to data owner so that he assigns an attribute set *S* to data user and adds the effective access time to the user. These attribute set and the master key are given as the input to this algorithm and it generates a private key S_{key} as the output. A common key is generated by the Diffie-Hellman key exchange protocol shared by the data user and owner. AES algorithm symmetrically encrypts the S_{Key} with the common key. This encrypted private key S_{Key} *′* will be stored in the SC for privacy.

***Decryption Algorithm*:** It is executed by the data user. Then data user performs decryption operation if and only if the time is within the valid access period. Data user obtains ciphertexts *C* and S_{Key}' from SC. The S_{Key} *′* will be decrypted by using the AES algorithm. This algorithm inputs the public key P_K, private key S_{Key} and ciphertext *C*. If S_{Key} satisfies the access policy *T*, data user can recover the key C_{key} of the encrypted document else the decryption will be failed. Data user will obtain the encrypted document E_{Ckey} (*M*) from the cloud, decrypts the encrypted document *M ′* by using key C_{key} and outputs the dM before data owner encrypts.

V. RESULTS

Figure 4 shows the graph of the run time of different algorithms vs the number of attributes. The graph of the literature algorithms [16] was shown in this figure with the red line. And graph of the proposed algorithm was shown in this figure with the green line. The execution time of the original algorithm increases with the attributes. The run time of our algorithm is almost consistent with the trend of the run time of the original algorithm. Since this design is based on the blockchain technology, it is more efficient and secure than all other algorithms.

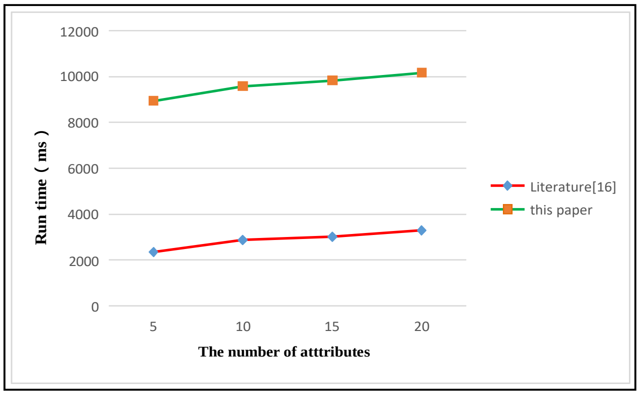

Fig. 4: Run times of different algorithms w.r.to number of attributes

VI. CONCLUSION

This presents a secured cloud architecture using the blockchain technology was designed and implemented. Here, the traditional algorithms for the security of clouds are replaced by the blockchain technology. The proposed algorithm’s run time is almost consistent with the trend of the original algorithm’s run time. We have adopted the blockchain technology in our design, so it is more efficient and secure than all other algorithms.

REFERENCES

[1]. Sukhodolskiy and S. Zapechnikov, “ A blockchain-based access control system for cloud storage, “ 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, p. p. 01575 - 01578.

[2]. S. Wang, X. Wang and Y. Zhang, “ A Secure Cloud Storage Framework With Access Control Based on Blockchain, “ in IEEE Access, vol. 7, p.p. 112713 - 112725, 2019.

[3]. L. Liu and B. Xu, “ Research on information security technology based on blockchain, “ 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, 2018, p. p. 0380 - 0384.

[4]. J. Li, Z. Liu, L. Chen, P. Chen and J. Wu, “ Blockchain-Based Security Architecture for Distributed Cloud Storage, “ 2017 IEEE International Symposium on Parallel and Distributed Processing with Ap. plications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA / IUCC), Guangzhou, 2017, p. p. 0408 - 0411.

[5]. S. Sayadi, S. Ben Rejeb and Z. Choukair, “ Blockchain Challenges and Security Schemes: A Survey, “ 2018 Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2018, p. p. 1-7.

[6]. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, “ The Blockchain as a Decentralized Security Framework [Future Directions], “ in IEEE Consumer Electronics Magazine, vol. 7, no. 2, p. p. 018 - 021, March 2018.

[7]. H. Xu, J. Cao, J. Zhang, L. Gong and Z. Gu, “ A Survey: Cloud Data Security Based on Blockchain Technology, “ 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), Hangzhou, China, 2019, p. p. 0618 - 0624.

[8].S. Ramamoorthy and B. Baranidharan, “ CloudBC-A Secure Cloud Data acess Management system, “ 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019, p. p. 0217 - 0220.

[9]. S. G. Sharma, L. Ahuja and D. P. Goyal, “ Building Secure Infrastructure for Cloud Computing Using Blockchain, “ 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, p. p. 01985 - 01988.

[10]. Y. Tang et al., “ ChainFS: Blockchain-Secured Cloud Storage, “ 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, p. p. 0987 - 0990.

[11]. N. Tapas, G. Merlino, F. Longo and A. Puliafito, “ Blockchain-Based Publicly Verifiable Cloud Storage, “ 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 2019, pp. 0381 - 0386.

[12]. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, “ NutBaaS: A Blockchain-as-a-Service Platform, “ in IEEE Access, vol. 7, p. p. 134422 - 134433, 2019.

[13]. Harshavardhan, T. Vijayakumar and S. R. Mugunthan, “ Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities, “ 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, p. p. 0408 - 0414.

[14]. S. Prianga, R. Sagana and E. Sharon, “ Evolutionary Survey On Data Security In Cloud Computing Using Blockchain, “ 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA), Pondicherry, 2018, p. p. 01 - 06.

[15] . N. Sanghi, R. Bhatnagar, G. Kaur and V. Jain, “ BlockCloud: Blockchain with Cloud Computing, “ 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, p. p. 0430 - 0434.

[16]. Zhang P, Chen Z, Liang K, et al. “ A Cloud-Based Access Control Scheme with User Revocation and Attribute Update “ , Part I, of the 21st Australasian Conference on Information Security and Privacy, Vol. 9722. Springer- Verlag NY, Inc. 2016: 0525 - 0540.