Cloudbc-To Ensure Data Integrity in Cloud Computing Environments

Amrutha S (amruthaselaveettil@gmail.com)
Amrita School of Arts & Sciences - Kochi Campus https://orcid.org/0000-0002-7999-3249
MAHESH A S
Amrita Vishwa Vidyapeetham - Kochi Campus: Amrita School of Arts & Sciences - Kochi Campus

Research Article

Keywords: cloud computing, attribute based encryption, online/offline, COVID19, Blockchain

Posted Date: May 17th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-511066/v1

CloudBC-to Ensure Data Integrity in Cloud Computing Environments

Amrutha S and Mahesh A S
Department of Computer Science and IT
Amrita School of Arts and Sciences, Kochi
Amrita Vishwa Vidyapeetham, India
amruthaselaveettil@gmail.com, asmahesh@asas.kh.amrita.edu

ABSTRACT

An outbreak of corona virus caused by a novel virus called SARS-CoV-2 occurred at the end of 2019. The unexpected outbreak and global spread of COVID19 indicate, the current global healthcare have limitations in addressing the crises for public safety. In this paper, we have studied to secure the COVID-19 patients' data. Data security and Storage Management becomes the most promising task in it, to manage it we use cloud computing. This leads to the unanswered questions related to the data security over the cloud data centres. The Proposed research work aims to protect the COVID-19 patient data, by cloud computing and implementing the new approach using blockchain technology. a novel secure Online/offline Decentralized Attribute Based Encryption for cloud. The proposed scheme reduces the online computation burden for data owners by completing the preprocessing computation as much as during the offline phase. The proposed scheme eliminates a major of computation overhead on user side by migrating the partial decryption computation to the cloud servers. The secure hash blocks are generated and which is maintained by the cloud storage devices to enhance the data security on the cloud. The block chains allow the user to trace malicious data access and modifications.

Keywords: *cloud computing, attribute based encryption, online/offline, COVID19, Blockchain;*

DECLARATION

I, **AMRUTHA S** hereby declare that the dissertation entitled "**CLOUDBC-TO ENSURE DATA INTEGRITY IN CLOUD COMPUTING ENVIRONMENTS**", submitted to the Amrita Vishwa Vidyapeetham, in partial fulfillment of the requirements for the award of the Master of Philosophy in COMPUTER SCIENCE & IT is an original and independent research work done by me during 2020-2021 under the supervision and guidance of Mahesh A S, Department of Computer Science & IT and it has not formed the basis for the award of any Degree / Diploma / Associate ship / Fellowship or other similar title to any candidate in any university.

Funding: Not applicable

Conflicts of interest/Competing interests : fulfillment of the requirements for the award of the Master of Philosophy and the supervision and guidance of Mahesh A S

Availability of data and material : kaggle, https://www.springernature.com/gp/authors/research-data-policy/data-availability-statements/12330880

Code availability: custom code

Authors' contributions: We combine the block chain technology to already existing system

Ethics approval: All procedures performed in studies were in accordance with the ethical standards of the institution

Consent to participate: Not applicable

Consent for publication : Not applicable

Date : 12/05/2021 AMRUTHA S

ACKNOWLEDGEMENT

My humble pranams at the lotus feet of **Mata Amritanandamayi Devi** who have been the guiding spirit in completing the research work.

I thank **God Almighty** for all his timely guidance and grace towards the accomplishment of the research work.

I express my deep sense of gratitude to our beloved Director **Dr.U. Krishnakumar** for his constant guidance and encouragement throughout the curriculum.I would like to express my sincere thanks to **Dr. Maya L Pai**, Head of the Department, for motivating us to undergo the dissertation programme.

I express my sincere gratitude towards our College Amrita School of Arts and Sciences, Kochi and to entire teaching and nonteaching faculty for encouraging me throughout my work.

I express my profound gratitude to my Research Guide **A. S. Mahesh**, Assistant Professor, Department of Computer Science & IT who have shown keen interest and helped me in completing the research work. It was a great experience to work under such qualified guide who made this research a great success.

Finally I thank each and every one who have assisted me in doing my research work.

AMRUTHA S

List of Abbreviations

1	COVID-19	coronavirus disease of 2019
2	WHO	World Health Organization
3	SARS	Severe acute respiratory syndrome
4	MERS	Middle East respiratory syndrome
5	SaaS	Software as a Service
6	PaaS	Platform as a Service
7	IaaS	. Infrastructure as a Service
8	ABE	Attribute Based Encryption
9	KP-ABE	Key-policy attribute-based encryption
10	CP-ABE	Ciphertext-Policy Attribute-Based Encryption
11	BC	Blockchian
12	PoW	Proof-of-Work
13	PK	Public Key
14	DO	Data Owner
15	CSP	Cloud Service Provider

16	DU	Data Users
17	GID	Global Identification Number
18	AA	Attribute Authorities
19	PS	Proxy Server
20	SHA256	Secure Hash Algorithm-256

1 Introduction

Corona virus disease has became a pandemic causing death toll around 3 lakhs and severe economic and political vaccum in major countries around the world [1]. The world is facing one of its most horrible crises regarding public health due to COVID-19, which was first identified in China in late December 2019 [1]. Infection of this virus is no longer limited to Wuhan. By January 2020 nine cases of COVID-19 infection have been stated in Thailand, Japan, Korea, USA, Vietnam, and Singapore through air travel is likely [2][3]. It has spread to almost all parts of the globe with major impacts on health and the economy. The WHO has warned that the COVID-19 pandemic is deteriorating worldwide [4] [5] [6] [7]. An important source for infecting this virus is asymptomatic carriers, With fewer research done on pandemic since SARS to COVID symptoms has been common such as fever, cough, sneezing etc. The infection rate of COVID-19 looks to be greater than that for the seasonal flu and MERS, with the kind of possible estimates covering the infection rates of SARS and Ebola. the healthcare industry quickly moved to improve its secure data sharing practices to improve research efforts and treatment development. For securely storing the data we choose could storage device.

Cloud Computing is an internet – based connection of server .It is used to store, manage and process data. The essential task for cloud computing is to compute the following: CPU, memory, storage, and network connectivity in cloud computing. The three types of services commonly offered by Cloud computing are [2] : 1. SaaS: SaaS applications are designed for end-users, delivered over the web. 2. PaaS: PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient 3 (IaaS): IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems. The study inculpating data must address security and privacy issues especially when delicate data is being handled.

In cloud computing, the data centres maintain the data storage devices which stores the data collected from the multiple user groups. The data stored on the cloud storage space maintains the high-level confidentiality of the data among the users. Still there exist malicious data access and modification among the genuine users. The lack of data access and modification details on the shared data leads to the inconsistent state among the group users. The lack of data access and modification details on the shared data leads to the inconsistent state among the group users. The requirement of group approved modification and shared data access services on the cloud storage model. All the group members part of this shared storage device should agree this data modification and access process ensure the confidentiality of the data.

The Block chain Technology is the one of the recent advancement in the field of data security. The technology makes use the strength of hash function and its unique values. The technology also allows the user to secure the data within the secure blocks. The attack over this shared medium can be monitored and traced using the block of chains. This chain connects number of computing node within in the community cloud network. The addition and deletion over this cloud networks should get the approval from other group users. It is impossible to regenerate the same hash value for the attackers.

The implementation of blockchain-based technology in the governments and healthcare industries will possibly improve the management of information protection and distribute health data while preserving data privacy and security [5]. Inherently we refer to the blockchain as a strategy of "decentralization." method, which means that information is stored not only on single server but an exchanged between many interconnected servers and stores shared data.

1.1 Objectives

This research aims to securely save the data of covid persistent securely in cloud using block chain technology. The significant contributions of this study are:

Migrate large number of encryption computation to the offline phase thereby reduce the computation overhead of data owner.

- Complex decryption computation are delegated to proxy and reduce the overhead of data user.
- Hash function is used to validate the ciphertext before the partial decryption.
- Sharing of data.
- Revocation key is generated in offline.
- Priority based revocation.

2 Literature Review

ABE introduced by Sahai and Waters [1], enables senders to encrypt a message such that only receivers that satisfy certain criteria can decrypt. There are mainly two types of attribute-based encryption schemes KP-ABE and CP-ABE. In KP-ABE, users' secret keys are generated based on an access tree. Access tree defines the privileges scope of the concerned user. Data are encrypted over a set of attributes. CP-ABE uses access trees to encrypt data. The users' secret keys are generated over a set of attributes. By comparing these two method Since focus on computation overhead CP-ABE is suitable.

In most ABE schemes, decryption keys are issued by a single central authority capable of verifying all the attributes/credentials issued for each user. Chase [2] first provided a multi-authority ABE scheme. In their basic scheme, each authority controls a set of attributes and decryption is possible only by a user who possesses at least a pre-specified number of attributes from each authority. Later, Chase and Chow [3], improved Chase's schemes in terms of security of encryption and user privacy.

Lewko and Waters' scheme [4] user can encrypt using any Boolean formula over attributes. Both Chase [8] and Lewko and Waters [4] use the concept of global identifier to replace the central authority. The global identifier links decryption keys issued to a user by different authorities. A number of schemes have since been proposed on privacy preserving multi-authority ABE. The efficient easy-ACCESS scheme [10] provides the advantages of shorter decryption keys, lower computation cost through delegation of decryption to a decryption service provider.

The idea of online/offline cryptographic algorithms was introduced by Even et al. [12] for digital signatures. This notion is applicable in a scenario where a resource-constrained device is required to perform cryptographic computations. Slower pre-computations are done during the offline phase so that faster, lighter and fewer computations need to be completed during the online phase. Pre-computations can be done while the device is being charged or not being otherwise used or can even be offloaded to more powerful devices. Guo et al. [11] proposed the first online-offline encryption scheme.

A new attempt to reduce the user's decryption overhead was made by Green et al. [12] with the help of outsourced computations. The user needs to provide a single transformation key to enable the cloud server to translate any ciphertext to a constant-sized El Gamal type ciphertext without the cloud knowing anything about the plaintext. He can then perform one simple exponentiation on the transformed ciphertext to obtain the plaintext. It was later shown in [13], that Green et al's method of outsourced decryption does not guarantee verifiability. A verifiable outsourced decryption scheme was proposed in [13] where the user can check efficiently whether the transformation was performed correctly. Balani and Ruj's scheme [15] enable partial outsourcing of decryption to a proxy server, ensuring the irrecoverability of plaintext by the proxy server.

User attributes are subject to periodic changes due to change in the work environment, location etc. [14]. That is, a user who was previously granted access to data may no longer qualify for the access. Unless previously allotted keys are updated and the user is revoked, the user may continue to access the data in spite of a change in his attributes. So, user revocation is a necessary and useful property for ABE schemes.

The encryption, revocation key generation and decryption phases are usually very costly and resource constrained devices are not suitable for performing such operations fast enough. The users can upload and download the data from cloud by incurring very little cost. As a solution to the costly encryption problem, divide the encryption phase into an offline phase and an online phase, such that, most of the costly operations are performed offline when the user does not immediately expect the encryption to be completed, the device is charging or otherwise not in use. The online phase has little computations so that users can get on with their work without the device's performance being affected in any respect. Costly decryption operations performed by data users are migrate to proxy server.

The proxy server, using a transformed decryption key, partially decrypts the ciphertext. The partial decryption process does not reveal any information to the malicious proxy server. Then, the data user needs to perform only a few simple operations to derive the final plaintext from the partially decrypted ciphertext. Similarly, revocation keys can be generated offline, with a few computations in the online phase for key transformation before they are given to the proxy server.

The adoption of blockchain on the cloud computing environment, upgrade the convenient cloud service to provide stronger security. The survey shows that majority of the research work focus on the improvement of blockchain from privacy and security perspectives. The survey helps the upcoming researcher can able to understand the security aspects related to the blockchain technology [5].

User anonymity can be ensured by blockchain method is used when saving the user information. Secure electronic wallet developed using the blockchain to minimize the issues related to the secure transactions. The improved security on the cloud based transaction established using this blockchain[6].

The BC not only used for implementing crypto currencies also it is used on PoW. BC uses a changeable PK to record the users' identity. Which provides an extra layer of privacy[7] to data .

3. Proposed Scheme

3.1 Problem Statement

To enhance the computation efficiency, the notation of ABE emerges, where complex computations were migrated to proxy to reduce the computation burden for users. To reduce the computation to encryption phase will divide the encryption to online and offline phase.

3.2 Proposed Statement

To enhance the security of the existing system Introducing this system to block chain technology. Combining the block chain and cloud computing will ensure the integrity and security of existing system. Also providing an hashing to ensure the integrity.

3.3 Architecture

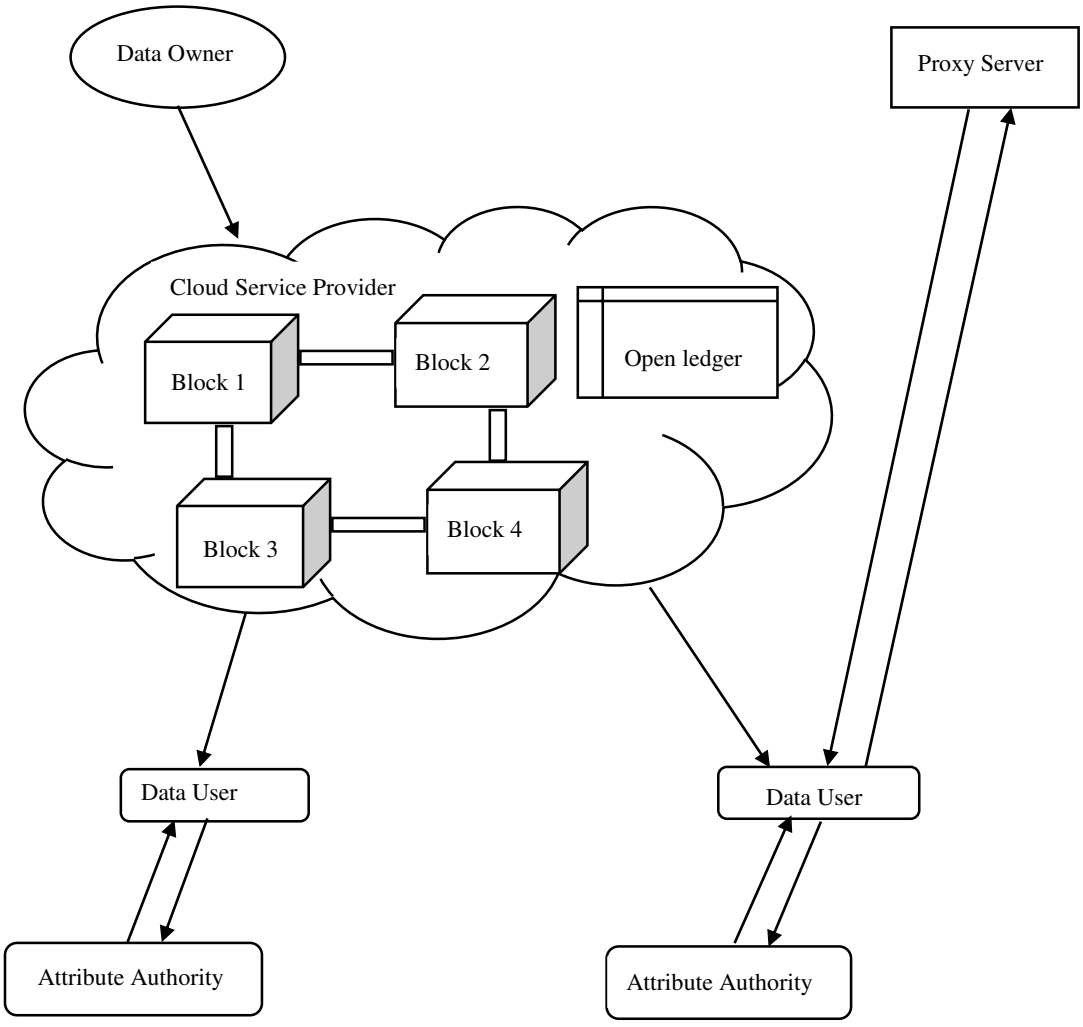

Figure 3-3 Architecture

4 Methodology

Data Owner: DO is an entity that owns data and uploads it to cloud storage after encrypting it. Data owners do not want the CSP to learn anything about their data and allows access to the data users whose attributes satisfy a given policy. Data owners may need to use resource-constrained devices to perform encryption on their data. All devices used by DO are assumed trusted.

Cloud Service Provider: Provides storage facilities for data belonging to data owners. The CSP is honest-but-curious. The CSP can try to find out information from the data stored in it but does not modified or deletes data.

Data Users: DU want to access data outsourced by the DO to the CSP. They can access this data if they satisfy a given policy. They must collect decryption keys corresponding to their attributes from Attribute Authorities. Data users are untrusted and may try to access data to which they are not authorized. They may also collude. Each data user has a GID, such as social security number or passport number that they have to submit to the attribute authorities in order to obtain the decryption keys. All devices used by DU for decryption are assumed trusted.

Attribute Authorities: There are more than one AA controlling different user attributes and generate the public key and decryption key corresponding to these attributes. Data users obtain their attributes and corresponding decryption keys from relevant attribute authorities on submitting their GID. For example, the Motor Vehicle's department may be an AA that certifies that a certain data user can drive. Similarly, a university may certify a data user to be a student of that university. Some AAs may be corrupted.

Proxy server: PS performs partial decryption of the encrypted cipher text. This helps in decreasing the decryption load on data user's devices without the proxy server knowing anything about the encrypted data. The proxy server may try to learn as much information as possible from the ciphertext but does not affect the correctness of the transformation. It can be either a part of the cloud server or a separate entity.

5 Results & Discussions

This encourages COVID-19 tested patients in full control over the data's privacy and sharing medical histories with consultants, hospitals, research institutions, and other stakeholders openly and securely.

5.1 Performance analysis

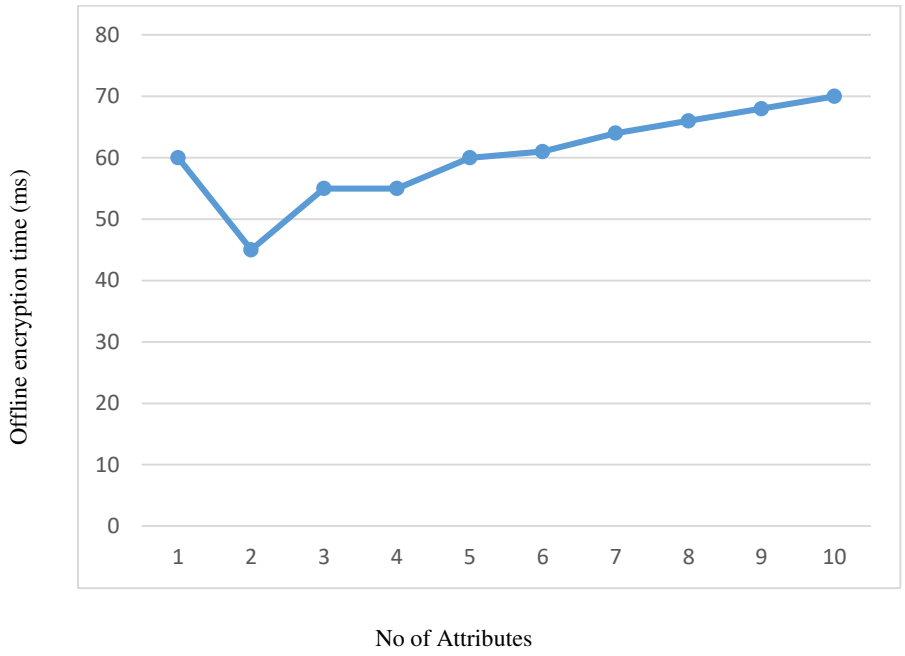

Figure 5.1 offline encryption time V/S number of attributes

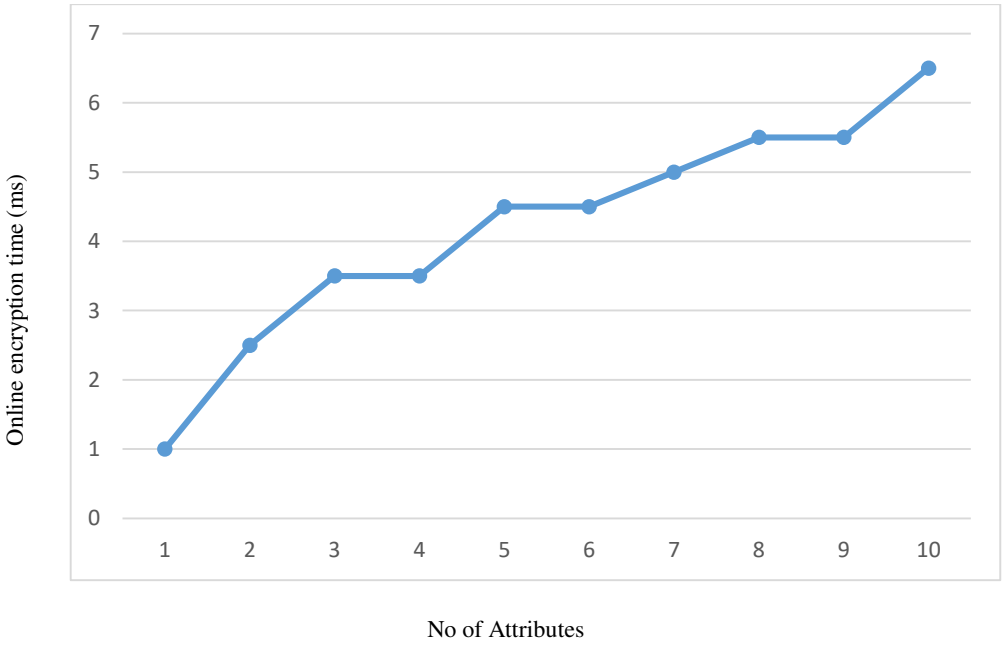

Figure 5.2 online encryption time V/S number of attributes

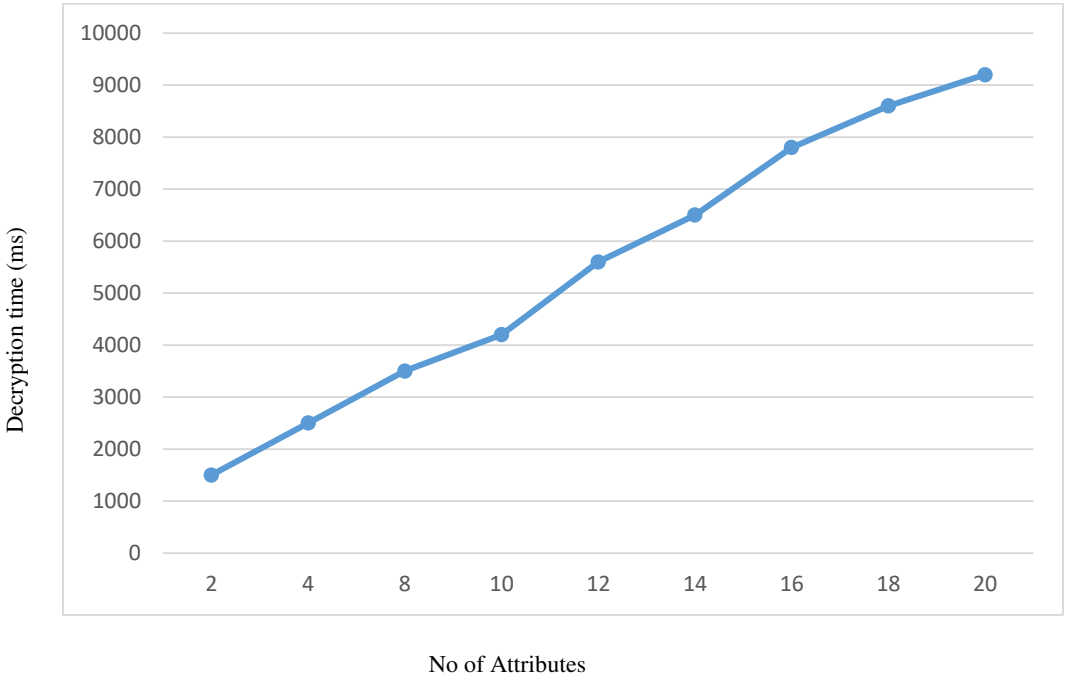

Figure 5.3 decryption time V/S number of attribute

6 Conclusion

In this paper, we consider blockchain technology's possible applications to globally identify infected or tested patients by a patient's unique identification. This proposed framework provides a health passport to COVID-19 tested patients. Its data refuse to modifications due to the nature of the blockchain data security. We aiming at addressing the issues of the computation efficiency and the weak security for resource constrained devices in cloud computing. To improve that we combined the cloud with block chain also Propose an Online/Offline Decentralized Attribute Based Encryption and SHA256 hashing. Proposed scheme minimizes the online computation for both encryption and decryption phases on owner side and user side. Moreover, the proposed scheme allows the proxy to validate the cipher texts before the partial decryption phase. In revocation phase saving a lot of computation overhead by aggregating data re-encryption. Revocation keys can be generated offline, with a few computations in the online phase for key transformation before they are given to the proxy server. Also Priority based revocation is possible.

In proposed system a priority based revocation is defined. Priority of data for each module will be different, so in future, the priority are defined over the data based for each module and revocation is done based on that.

References

[1] S. Ramamoorthy, B.Baranidharan, Associate Professor, Department of CSE,SRM Institute of Science and Technology, , “CloudBC-A Secure Cloud Data acess Management system”, 2019

[2] Dr.B. Ravishankar, Prateek Kulkarni, and Vishnudas M V, Professor, IEM Department, B.M.S. College of Engineering, Basavangudi, “Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments”,2020

[3] Nikita Sanghi, Rupali Bhatnagar, Gaganjot Kaur, department of CST, Manav Rachna University, Faridabad ,India, Vinay Jain, Accendere Knowledge Management, Services Pvt. Ltd. , India, “BlockCloud: Blockchain with Cloud Computing”, International Conference on Advances in Computing, Communication Control and Networking 2018

[4] Proof of Work vs Proof of Stake: Basic Mining Guide, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake

[5] Cloud computing, https://en.wikipedia.org/wiki/Cloud_computing

[6] Khan G, Sheek-Hussein M, Al Suwaidi AR, Idris K, Abu-Zidan FM. Novel coronavirus pandemic: A global health threat. Turk J Emerg Med 2020;20:55-62

[7] WHO Novel coronavirus – Republic of Korea (ex-China). Geneva: World Health Organization. 2020. https://www.who.int/csr/don/21- january-2020-novel-coronavirus-republic-of-korea-ex-china/en/

[8] US Centers for Disease Control and Prevention First travel-related case of 2019 novel coronavirus detected in United States. Atlanta, GA: US Centers for Disease Control and Prevention. 2020. https://www.cdc.gov/media/ releases/2020/p0121-novel-coronavirustravel-case.html

[9] Amrutha s and Prof .(Dr) Vinodu george, Department of Computer Science, L B S College of Engineering Kasaragod, India, “online/offline decentralized attribute based encryption for mobile clouds”, international conference on advances in security and computing- ICASC 2019

[10] Secure Online/Offline Multi-Authority Attribute-Based Encryption for Resource constrained Device in Cloud Computing, Jiaye Shao, Yanqin Zhu, Qijin Ji, 2018 IEEE Sharma, P.K., Chen, M.Y. and Park, J.H., 2018. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, pp.115-124.

[11] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., 2016. Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), p.e0163477.

[12] Park, J.H. and Park, J.H., 2017. Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9(8), p.164.

[13] Miraz, M.H. and Ali, M., 2018. Applications of Blockchain Technology beyond Cryptocurrency. arXiv preprint arXiv:1801.03528.

[14] Ming, Z., Yang, S., Li, Q., Wang, D., Xu, M., Xu, K. and Cui, L Blockcloud: A Blockchain-based Service-centric Network Stack.

[15] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.

[16] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain. Information Security Research., 12: 1090-1097.

[17] Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.

[18] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD. Advances in Eurocrypt., 3494: 1-18.

[19] Barkatullah J, Hanke T. Goldstrike 1: CoinTerra‘s First-Generation Cryptocurrency Mining Processor for Bitcoin. Micro, IEEE. 2015; 35(2):68–76. doi: 10.1109/MM.2015.13

[20] Garay J, Kiayias A, Leonardos N. The Bitcoin Backbone Protocol: Analysis and Applications. In:Oswald E, Fischlin M, editors. Advances in Cryptology— EUROCRYPT 2015. vol. 9057 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2015. p. 281–310. Available from: http://dx.doi.org/10.1007/978-3-662- 46803-6_10.

Figures

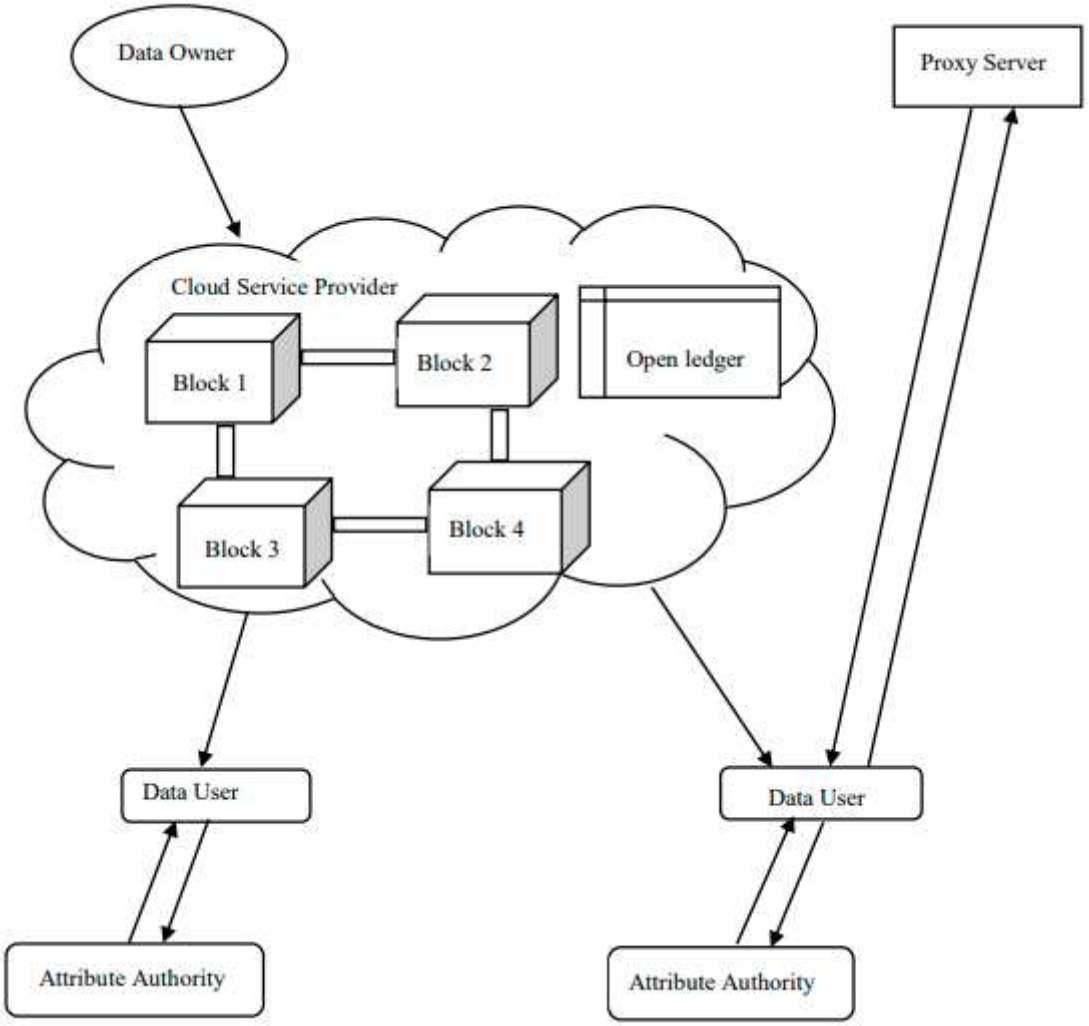

Figure 1

Architecture

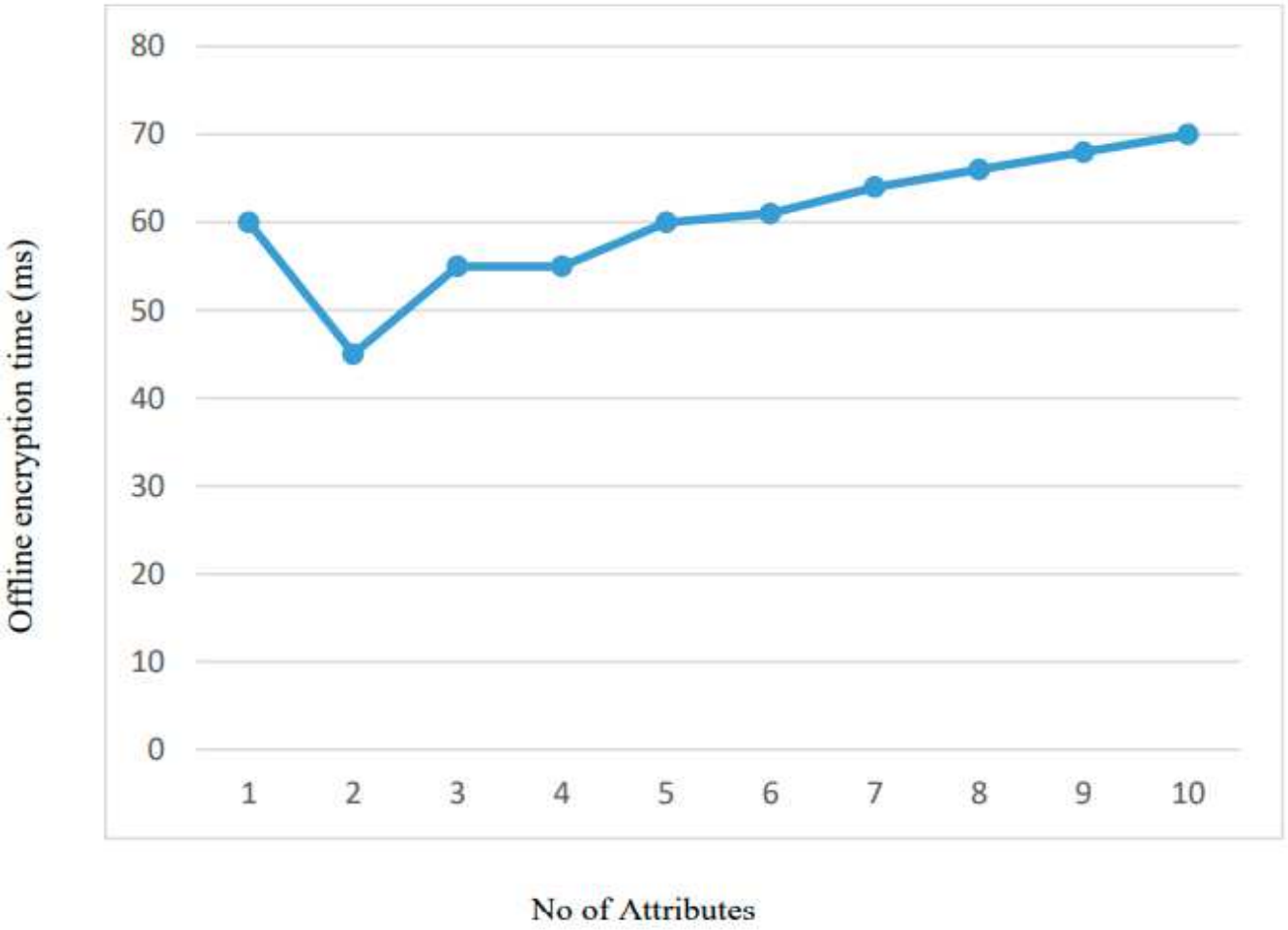

Figure 2

offline encryption time V/S number of attributes

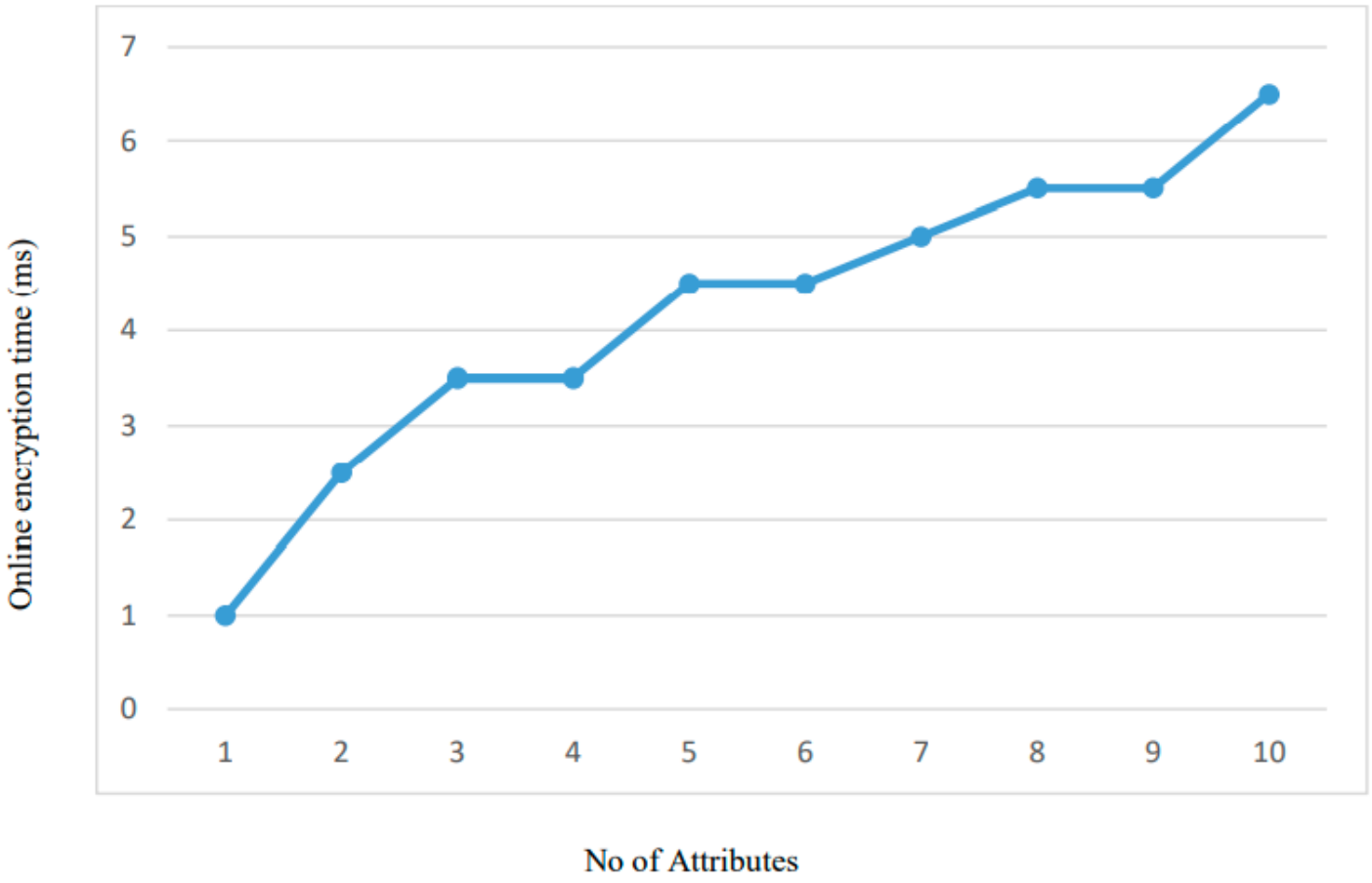

Figure 3

online encryption time V/S number of attributes

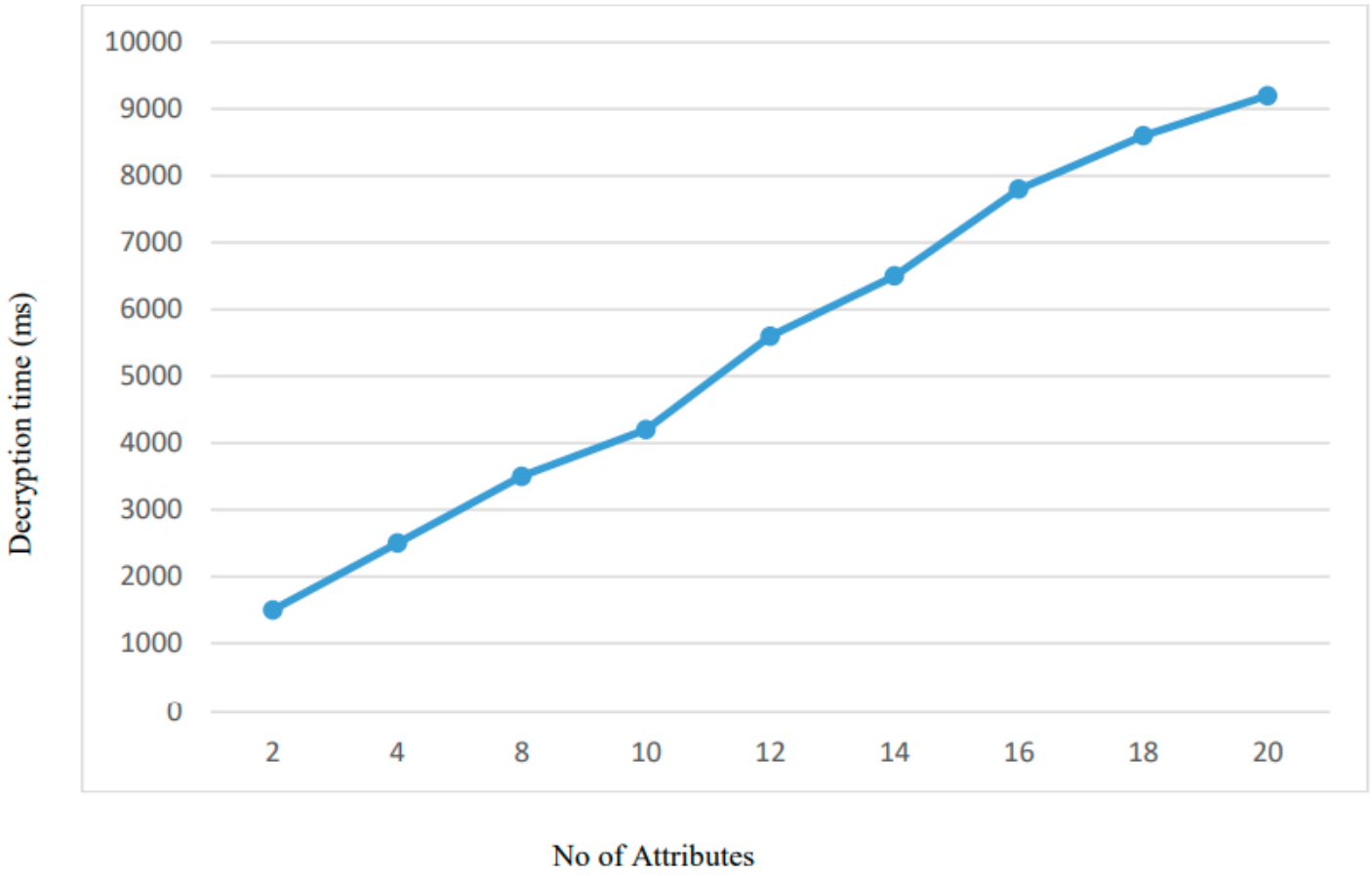

Figure 4

decryption time V/S number of attribute