International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Managing Cloud Data Integrity and Access Control Mechanism through Blockchain

Rushabh Rajendra Desarda, Nishant Ganesh Chavan, Amit Gunaji Chaure, Pankaj Ramanlal Gandhi, Prof. S. E. Ingale

Computer Department, MES College of Engineering, Pune, Maharashtra, India

ABSTRACT

Ever since the introduction of the internet platform there has been a significant increase in the number of services that utilize the internet paradigm. one such service is the cloud storage platform. The cloud is a collection of a large number of services that leverage the internet platform to provide users with increased convenience for performing day to day activities. The cloud storage platform is an innovative concept that allows the user to store their data on the cloud platform to enable increased convenience for the users as the data can be accessed on any device with just an internet connection. But the problem arises when the data is supposed to be accessed by several entities such as the cloud admin along with the auditors and other users while maintaining the security of the data stored. Therefore, there is a need for an efficient and secure access control mechanism that needs to be implemented on the cloud storage platform. The proposed methodology in this publication implements Reverse Circle Cipher along with the introduction of the Blockchain Distributed platform for the creation of an effective access control and integrity management technique on the cloud storage platform.

KEYWORDS: *Cloud Computing, Blockchain, Reverse Circle Cipher, Access control mechanism*

***How to cite this paper**:* Rushabh Rajendra Desarda | Nishant Ganesh Chavan | Amit Gunaji Chaure | Pankaj Ramanlal Gandhi | Prof. S. E. Ingale "Managing Cloud Data Integrity and Access Control Mechanism through Blockchain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.1158-1163, URL: www.ijtsrd.com/papers/ijtsrd30795.pdf

IJTSRD30795

I. INTRODUCTION

Knowledge is one of the most important aspects that has enabled large scale technological advancement in the world. Knowledge in the most sense is equivalent to the amount of data that is being stored and transferred to the upcoming generation. Ever since the invention of the internet platform, there has been an increase in the amount of data that is being generated all over the world. The internet paradigm is one of the most useful communication networks that have been facilitating the transfer of data and information across large distances. There are a large number of websites at portals that also provide valuable information for the people to access over the internet platform.

The proliferation of the internet also gives birth to an innovative platform called the cloud. The cloud platform is a novel concept that has arisen due to the inherent ubiquity of the internet. The cloud platform is a misnomer as it was coined after the various diagrams and representation in the early stages of the internet depicted it in the form of a cloud. thus, the name stuck and has been utilized for describing various services that are provided through the use of the internet platform. The cloud platform facilitates various services that have the internet as the backbone providing the connection between the user and the services on a remote server. The cloud provides a variety of services such as infrastructure as a service platform as a service and software as a service Most popular services that are utilized in the cloud is the cloud storage. Cloud storage is Highly popular as it provides for reliability and ease of Access for the data that is stored in the cloud. Many major companies and individuals have been utilizing cloud storage for ubiquitous and maintenance-free storage and access to the data. The cloud is also referred to as a mobile storage as the data stored on the cloud can be accessed anywhere in the world and on any device as long as there is an Internet connection available. Therefore, many corporations and individuals can save up valuable resources in setting up and maintaining local storage which has Limited availability and is highly volatile if not managed properly. Therefore, the platform of cloud storage is a highly useful platform that has quickly gained a lot of users due to its innovative and useful methodology.

To provide unique ways to reach the cloud platform aggregates the user data onto a remote server on the cloud. This facilitates easy access to data from anywhere in the world. But most of the time it is is highly valuable or sensitive data of the individual or organizations that are stored on the cloud platform. This sensitive data may contain valuable documents and other personally sensitive information that is stored on the cloud for easy access. This is a highly dangerous proposition as the user gives up control of the data to the cloud provider and is at the Mercy of their security implementations. Therefore, there is a need to implement an effective security system to safeguard the data on the cloud platform. The date on the cloud is highly susceptible to attacks in various forms other users, the data owners, or the auditors try to access the data on the cloud.

Therefore, to provide security on the cloud and implement an effective access control mechanism one of the best approaches for this is the implementation of the blockchain platform and the reverse circle Cipher mechanism. The blockchain platform was invented by a group of scientists in late 1990 as a means of achieving a distributed ledger system that can be utilized for the implementation of a digital notary. It was not as popular at that time and was effectively forgotten by many researchers after a period of time. The blockchain platform got immense popularity when it was utilized to create a crypto currency called Bitcoin. Due to the tamper-proof security provided by the distributed blockchain network, it was the best application for the creation of a crypto currency. This renewed interest in this platform sparked various researches for the utilization of the blockchain platform for implementing a tamper-proof mechanism based on a distributed network.

The RCC or reverse circle cipher is a very unique and innovative encryption mechanism. Reverse circle cipher has been extensively used to provide network as well as data security which has been highly difficult for many cryptographic algorithms to achieve this level of Universal application. This is due to the fact that there are specialized algorithms that are used for different applications such as advanced encryption standard or AES is used extensively for personal data protection and are not as useful for the purpose of protecting real-time data in a network. On the other hand, for the implementation of effective network security, RSA is utilized extensively but has an increased space and time complexity that is not suitable for large scale applications in both situations. Therefore, the reverse circle cipher utilizes reversal transposition and circular substitution that effectively diffusion and confusion to its benefit while safeguarding the data on a network efficiently. The combination of the blockchain and RCC is a very unique combination that can efficiently provide an effective access control mechanism to save guard the data on the cloud platform.

This research paper dedicates section 2 for analysis of past work as literature survey, section 3 deeply elaborates the proposed technique and whereas section 4 evaluates the performance of the system and finally section 5 concludes the paper with traces of future enhancement.

II. LITERATURE SURVEY

S. Wang explains that there is an increasing number of individuals and Enterprises that have been utilizing the cloud storage platform for outsourcing their data. This is because the cloud platform can provide a solution to a lot of problems such as the one faced with maintaining the local storage options [1]. That the authors in this paper have provided data deduplication techniques that can save a lot of storage of the cloud system. The experimental results conclude that the proposed methodology significantly reduces the storage cost of the cloud server.

Qiwu Z expresses the various problems that are related to cloud storage especially concerning the security of the cloud against forking attacks. These are the type of attacks that can cause large scale data breach which can put the sensitive data of the clients at risk and also lead to the reduction of trust between the cloud platform and the client [2]. Therefore, the authors in this paper propose an effective implementation of the blockchain framework for file operation logging and key distribution that significantly improve resilience against forking attacks. The experimental results conclude that the system performance with the implementation of this Framework has achieved very low overheads.

K. Wang introduces the fact that data is one of the most important resources to perform mining and artificial intelligence algorithms. Which applications requires a lot of data that is not easily available and is distributed everywhere on the internet. for this purpose, various data stakeholders aggregate the data according to the application and provide for utilization in these various algorithms [3]. This is a very sensitive task as the data might contain some sensitive information therefore the blockchain platform is utilized to enable a tamper-proof nature and improve the security. The experimental results conclude that SecNet is highly useful and improved security by a large margin.

N. Tapas [4] elaborate on the large-scale adoption of cloud storage in various applications such as machine learning data mining and other IoT solutions. Cloud storage has increased user base due to its growing popularity that has been steadily used by various businesses and individuals. This is a problematic occurrence as the data might contain some sensitive information that it needs to be protected at all times. Therefore, the authors in this paper propose publicly verifiable cloud storage based on the blockchain platform which enables tamper-proof security to the cloud storage effectively.

T. Gabriel discusses the various advantages and disadvantages that are faced when utilizing a decentralized solution for renewable energy sources. Most of the renewable energy has been transformed from a monolithic architecture to a decentralized one which has created a series of problems that need to be solved effectively. Therefore, the authors propose the implementation of the blockchain technology in this decentralized architecture to achieve increase security by neighboring the tamper-proof nature of this technology [5]. The experimental results conclude that the proposed methodology achieves satisfactory results.

I. Sukhodolskiy explains that the cloud storage platform has been utilized extensively by various users for securely storing the information and data to be able to easily accessible anywhere. Most of the time multiple users are accessing the same amount of data on the cloud at the same time this is a very normal occurrence at large corporations [6]. But this causes a problem with the security of the data which can be compromised easily. The food hotels in this Publication implement and access control system that is based on the blockchain platform. The experimental results conclude that the smart contracts in the blockchain platform can provide a secure and safe access control mechanism.

M. Kumar [7] describe the current era as the era that is governed by information technology. There is a lot of information on the internet and an increasing amount of data is being created every day. This provides a very major challenge for various monitoring systems attached to the management and monitoring of the data. the main challenge is providing security to this data as there are a lot of attackers with malicious intent trying to create a data breach. To ameliorate this, affect the authors in this paper have proposed an effective technique for securing log storage on the cloud infrastructure by the implementation of the blockchain platform.

H. Zhu introduces the various problems faced by the increasing size of the user base that has been utilizing the cloud storage platform for various purposes. As the user base increases the traffic of the data in the cloud platform increases significantly. Therefore, to provide a quality service to every user on the platform becomes highly difficult [8]. To provide a solution to this effect the authors in this paper have proposed the utilization of the blockchain platform for or solving the resource scheduling problem in a decentralized manner. the experimental results conclude that the cloud resources schedule proposed in this paper performs exceptionally well.

S. Ramamoorthy elaborates on the access control problem that is associated with large organizations using the cloud storage platform with several employees simultaneously. This kind of usage creates a lot of loopholes that can be exploited by an attacker to gain unauthorized access to sensitive data [9]. Therefore, the development of a secure access management system is the need of the hour for a cloud storage platform. therefore, doctors in this paper propose the utilization of the blockchain platform for the implementation of a secure and efficient access management system. The performance evaluation concludes that the proposed methodology performs as expected.

X. Yang discusses the problems that have been faced by online voting platforms that have been implemented in various countries all over the world. The most important concern is the security of the voting data that is being utilized in the cloud platform. Therefore, to enable increase security to the platform the authors in this paper provide the utilization of homomorphic encryption along with rank choice online voting system which addresses all of these issues. The performance evaluation of the proposed methodology reveals that the method has significantly improved security in comparison to the conventional approaches. [10]

Keke Gai expresses that the cloud computing platform has increasingly become a part of life for the majority of the people. This is because the cloud platform is highly convenient and low-cost alternative various services [11]. This has prompted the increase of various cloud data centers that have been utilized to provide these services to this increasing user base. This also includes increasing challenges that have been related to the access control mechanisms on these data centers, therefore, the authors in this Publication elaborate on the implementation of the blockchain platform for the re-engineering of various cloud data centers.

Jiaxing Li states that there has been large scale development in various industries all over the world which has significantly prompted the increase in the demands for storage and accessibility on a large scale [12]. Most of these issues have been addressed by the implementation of the cloud platform that allows for all of these challenges to be easily overcome. But the challenges that remain are related to the security of the cloud storage platforms as increasing numbers of attacks have been performed on this framework. Therefore, to provide a solution to all of these problems the authors propose the implementation of a distributed cloud storage with the help of the blockchain platform. The experimental results indicate that the blockchain platform significantly improves the security of the cloud storage paradigm.

III. PROPOSED METHODOLOGY

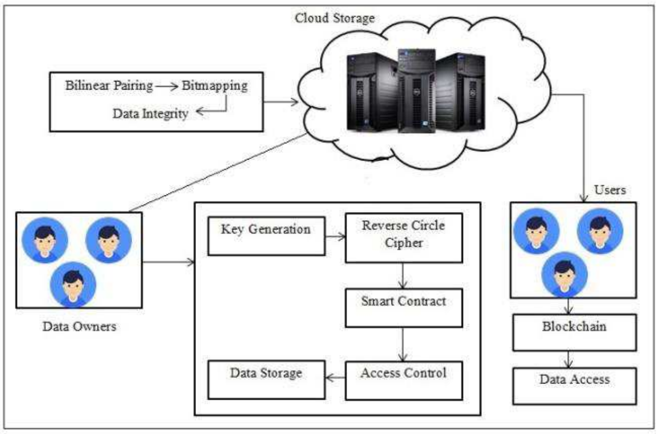

Figure 1: Overview of the proposed model

The Proposed model of Data Integrity and access control mechanism is depicted in the above mentioned Figure 1. The steps that are taken to implement the proposed model are being elaborate below.

Step 1: Cloud setup and User Registration – The Proposed model is incorporated using the Java programming language. A standalone system is being developed using the Swing framework for an interactive user interface. A facility is being provided to the user to sign up into the model, as the proposed model accepts the user credentials for the registration purpose, then the entire user data is being stored in the database along with a unique Signature key. This signature key is generated for the entered user credentials for only one time.

Preliminarily all the user credentials are being concatenated and then are fed to the MD5 Hashing algorithm to generate a unique hash key. From this hash key 7 character unique signature key is being generated for a user to store along with his credentials in the database. This signature key is being made as concrete so that it cannot be modified by any of the user operations and remain as the unique credential with the user id. The formation of the signature key is depicted in the below shown algorithm 1.

For the efficient implementation of the proposed model a public cloud Dropbox is being used. The open source API of the Dropbox cloud is being efficiently integrated in the Netbeans 8.0 IDE using the API keys of the specific user ID.

ALGORITHM 1: Key Generation

```
//Input: MD5 Hash Key MHK
//Output: Key
1: Start
```

```
KEY =" "
IND= MHK length MOD 7
    FOR i=0 to KEY Length <7
        i=i+( IND +1)
            IF ( i< MHK length)
            KEY=KEY+ MHK[i]
            MHK = MKH >> 1
            ELSE
            i=0
            END ELSE
        END FOR
    return KEY
Stop
```

Step 2: Reverse Circle cipher- This is the step that eventually adds more security for the uploading data into the cloud. The selected file by the user is read into the array of bytes F[ ]. Each of the byte of the array is added with the key value. Then this array of bytes is blocked into size of 10. Then each block is rotated based on the normalized rotation factor of the block index. After this, these rotated bytes are stored into another byte array to write as an encrypted file. The working model of this encryption algorithm is depicted in the algorithm 2.

ALGORITHM 2: Reverse Circle Cipher

```
//Input: File Byte Array F[ ] ,K as Key
//Output: Encrypted Bytes E[ ]
Start
$L_{ST}$ = NULL [ List] , N=10 ,Count=1
ind=0
    FOR i=0 to Size of F
            $L_{ST}$ = $L_{ST}$ + ( F[i]+key)
            IF ($L_{ST}$ SIZE =N )
            Count=Count MOD N
    FOR j=0 to Size of Count
    $L_{ST}$= $L_{ST}$>>1
    END FOR
            FOR k=0 to Size of $L_{ST}$
            E[ ind++]= $L_{ST}$[k]
            END FOR
    Count++
    $L_{ST}$=NULL
    END IF
END FOR
            FOR k=0 to Size of $L_{ST}$
            E[ ind++]= $L_{ST}$[k]
            END FOR
    return E
Stop
```

Step 3: Smart Contract Access Control and Blockchain Creation - This is step which eventually laid the foundation for the gross security of the stored data. Here as the each uploading file is encrypted at the user end, then its hash key is used to estimate the 7 character unique key using the algorithm 1. And this unique 7 character of the file hash key is known as the head key and the file byte array is known as the block body. This head key is being mixed with the next file block body to generate its head key. This way it leads to the formation of a blockchain efficiently.

The very first file uses the user signature as the previous key to generate its head key to start the process of smart contract and thereby blockchain process.

Step 4: Data Integrity Evaluation - The data integrity of the stored data in the cloud is the necessary task to ensure the stored data at the cloud end is secured. For this purpose the proposed model considers the entire file that is being uploaded to the cloud. And then each of the file byte data is being downloaded to create the block body and the respective head keys.

Each head obtained key from the cloud data are matched with the respective head keys of the file stored in the database on the client end machine.

Any dissimilarity in the head keys leads to declaring as the violation of the integrity of the data at the cloud storage end. This process is continuously being watched till the user terminates the same. And the simultaneous reports are being generated for the data integrity compromisation on the interactive user interface along with the details like violated date and time.

IV. RESULT AND DISCUSSIONS

The proposed methodology implemented for enabling effective and secure cloud access control through the use of the Reverse Circle Cipher has been coded in using the NetBeans IDE in the Java Programming language. The machine utilized for the development process executes on a Windows Operating System equipped with an Intel Core i5 processor assisted by 500 GB of a hard drive as storage and 4GB of RAM. The database responsibilities are handled by the MySQL database.and The DropBox public cloud is being utilized for the purpose of the storage and Maintaining the data integrity of cloud storage data.

The presented technique has been evaluated extensively for its execution performance on various parameters. The experimental testing and their results have been given below.

4.1. Encryption and Decryption Time performance

The presented system is put through extensive encryption and decryption performance time measurement and the results of the experimentation are listed in Table 1 below.

Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
17	2	3
1709	15	13
2605	32	30
3214	49	43
4898	56	59
5731	66	63
6501	69	65
8196	79	80
8756	80	76
9789	98	99

Table 1: Encryption and Decryption time performance

Figure 2 above, illustrates that the encryption and decryption timings are not related to the increasing number of characters in a directly proportional relationship. This type of nonlinear correlation is an indication of a good performance metric achieved by the encryption and decryption module which has been executing as intended in this implementation with very high accuracy.

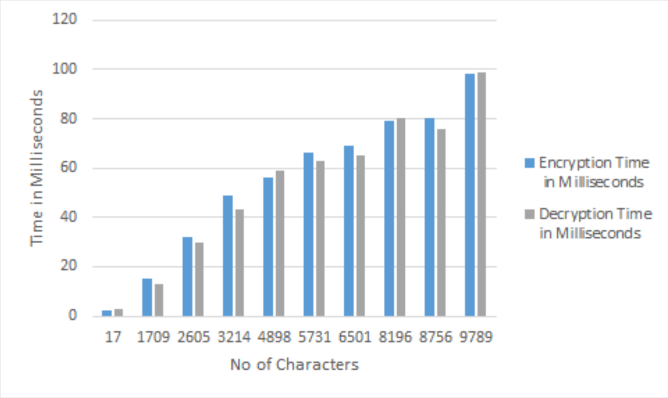

Figure 2: Encryption and Decryption Time

4.2. Error Probability of Message Decoding

The Reverse Circle Cipher used in this methodology is tested for its execution and the probability of error by utilizing the message decoding feature of this algorithm. Extensive experimentation involving the various runs of the module for an increasing number of the characters is measured. The measure of the error probability decoding of the Reverse circle cipher and results obtained are tabulated in Table 2 below.

Number of Characters to be used for	Error Probability after RCC (in %)
2	0
5	0
7	0
8	0
11	0
12	0
15	0
19	0
21	0
25	0

Table 2: Error probability after message Decoding using RCC reading

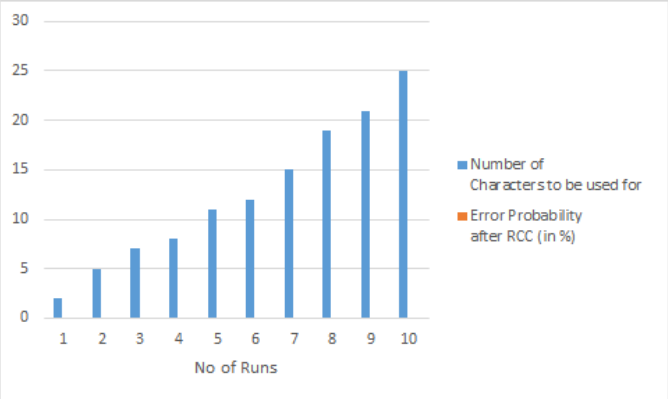

Figure 3: Error probability after message Decoding using RCC reading

Methodology	Error Probabiliity Rate in %
RCC	0
ECC	0

Table 3: Error probability after message Decoding using RCC and ECC

The graph plotted in figure no 3 illustrates that the presented Reverse Circle Cipher module doesn't encounter any error probability in the message decoding approach applied in the proposed methodology. And when the result is contrasted with that of the ECC (Elliptical Curve Cryptography) mentioned in [13], then the presented system has encountered that the error probability of both approaches is 0. And hence the presented system is demonstrated to acquire the best error probability rate for message decoding through the utilization of the Reverse Circle Cipher algorithm.

V. CONCLUSION AND FUTURE SCOPE

The proposed methodology for the purpose of implementing an innovative and secure access control mechanism on the data stored on the cloud storage platform has been outlined in this research. The cloud storage platform has been increasing in popularity exponentially nowadays, as more individuals and organizations have been adopting this platform for the increased convenience and economical options offered by the platform. This increase in the users also requires extensive security on the platform where multiple users are accessing the data at the same time. Therefore, to ameliorate this effect a novel approach towards implementing an access control mechanism is detailed in this paper that utilizes the Reverse Circle Cipher along with the introduction of the Distributed framework of the Blockchain platform for providing an effective access control mechanism. The performance metrics of the presented metrics were evaluated for their errors and encryption performance extensively. The experimental results achieved indicate that the methodology outlined in this research improves upon the traditional access control mechanisms by a large margin.

For the Future Research approach, the proposed system can be scaled up to be deployed in a distributed environment on the cloud platform. The approach can also be developed as a mobile application that can be easily accessible to users.

References:

[1] Shangping Wang, Yuying Wang, And Yaling Zhang," Blockchain-based fair payment protocol for deduplication cloud storage system "Digital Object Identifier 10.1109/ACCESS. Doi Number. 2019

[2] Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla," ChainFS: Blockchain-Secured Cloud Storage", IEEE 11th International Conference on Cloud Computing 2018

[3] Kai Wang, Jiaqing Dong, Ying Wang," Securing Data with Blockchain and AI" Digital Object Identifier 10.1109/ACCESS.2921555 2019

[4] Nachiket Tapas, Giovanni Merlino, Francesco Longo, Antonio Puliafito," Blockchain-based Publicly Verifiable

Cloud Storage" IEEE International Conference on Smart Computing SMARTCOMP 2019

[5] Tudor Gabriel, Andrei Cornel Cristian, Madalina Arhip-Calin, Alexandru Zamfirescu," Cloud Storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Blockchain technology" 978-1-7281-3349-2/19©IEEE 2019

[6] Ilya Sukhodolskiy, Sergey Zapechnikov," A Blockchain-Based Access Control System for Cloud Storage" 978-1-5386-4340-2/18 IEEE 2018

[7] Dr. Manish Kumar, Ashish Kumar Singh, Dr. T V Suresh Kumar," Secure Log Storage Using Blockchain and Cloud Infrastructure" July 10-12, IISC, Bengaluru 2018

[8] He Zhu, Yichuan Wang, Xinhong Hei, Wenjiang Ji, Li Zhang," A Blockchain-based Decentralized Cloud Resource Scheduling Architecture" International Conference on Networking and Network Applications 2018

[9] 1S. Ramamoorthy, B. Baranidharan," CloudBC-A Secure Cloud Data Access Management system" 978-1-5386-9371-1/19/ IEEE 2019

[10] Xuechao yang, Xun yi1, Surya Nepal, Andrei kelarev, and Fengling Han," A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption" Digital Object Identifier 10.1109/ACCESS.2817518 2018

[11] Keke Gai, Kim-Kwang Raymond, Liehuang Zhu," Blockchain-Enabled Reengineering of Cloud Datacenters" Co-published by the IEEE CS and IEEE ComSoc November/December 2018 2325-6095/2018

[12] Jiaxing Li, Zhusong Liu, Long Chen, Pinghua Chen, Jigang Wu," Blockchain-based Security Architecture for Distributed Cloud Storage" IEEE International Symposium on Parallel and Distributed Processing with Applications 2017

[13] Iuliia Tkachenko, William Puech, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard, "Two-Level QR Code for Private Message Sharing and Document Authentication", IEEE Transactions on Information Forensics and Security, Vol. 11, No. 3, March 2016.