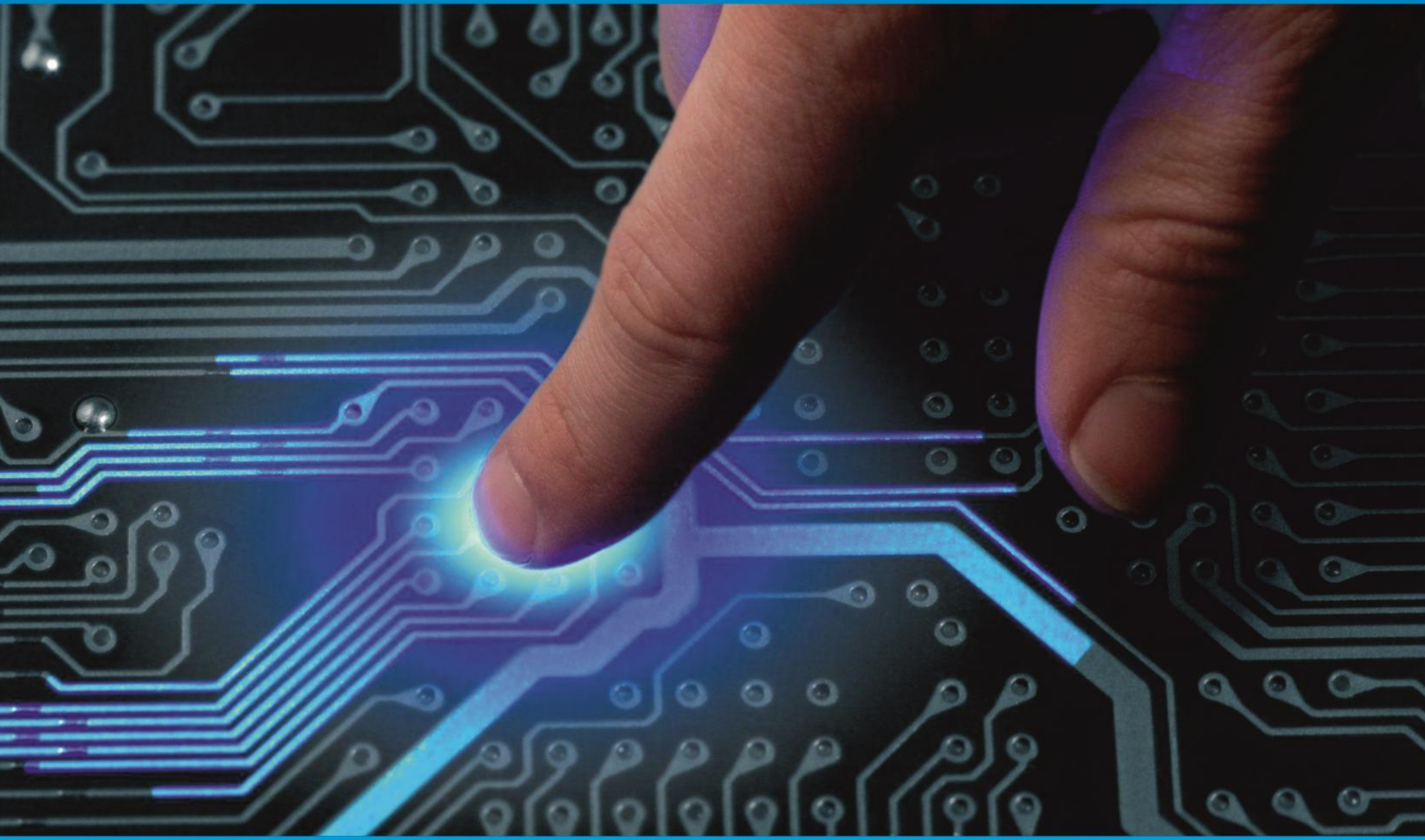
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

☎ 9940 572 462 | 6381 907 438 | ✉ ijircce@gmail.com | @ www.ijircce.com

Enabling Search over Encrypted data and Data Integrity Evaluation in Cloud

Pratiksha Dhavale, Pratiksha Raut, Neelam Divekar, Aishwarya Kadam, Nagaraju Bogiri

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

UG Student, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

ABSTRACT: There is an increase in the attention towards security detail of the data of individuals as well as organizations in the recent years. This has been attributed to the increased cyber threats that have been successful in performing data thefts and data leakage that have been highly problematic for a number of individuals and organizations. This is due to the fact that a large number organizations and individuals have personally identifiable data that is being uploaded on remote servers in the public cloud environments. The use of cloud services has been due to the increased efficiency and ubiquity that is offered through the cloud platform. Usually the data to be protected is encrypted to convert it into a format that even if the storage is compromised, the attacker cannot get access to the data. But on the cloud platform, the encryption of the data breaks certain searching capabilities which can be problematic to search this encrypted data on the public cloud. Therefore, a reliable and highly efficient scheme for searching over encrypted data on the cloud platform has been proposed in this research article. The approach utilizes the Reverse Circle Cipher encryption and implements the Tiled bitmap approach to provide searching as well as encryption thereby protecting the data on the cloud.

KEYWORDS: Cloud Computing, Reverse Circle Cipher, Search Over Encrypted Data, Tiled Bitmap Algorithm.

I. INTRODUCTION

The collection and storage of data have been one of the fundamental concepts that have driven the wheels of technological advancement in the world. Data is one of the most essential commodities that has been utilized to facilitate a large number of different inventions and discoveries that have slowly but significantly had an impact on the landscape of our planet. One of the earliest forms of data storage was in the form of songs and other stories that were remembered and told to the next generations to help preserve the knowledge. This was due to the lack of any storage mechanism that would allow for a much easier retrieval therefore, data were restricted to word of mouth.

This changed significantly throughout the advancement of the human race, which led to the first instances of paintings. This is due to the fact that the pictorial representation of information is easier to understand by the brain as well as useful for the purpose of efficient retrieval. Such paintings were used to train the younger generations in the art of hunting and cooperating with other members of the tribe in acquiring food and shelter. The cave paintings were also a form of relaxation and served a dual purpose of education along with the other storytellers. This was how the information was utilized for a large number of years until the human started agriculture.

The early humans transitioned from a hunter-gatherer which roamed the lands like nomads to a purely agrarian society that started settlements and grew crops and other useful food and clothing items. This was the time when the stone tablets were used to store important information. Carving the stone was a tedious process that took a long time; therefore, only highly valuable information was stored on such tablets. This was the way information and data were preserved and retrieved for a long time. This was replaced by the use of papyrus in the early form of the paper that was used to mark the relevant information.

The papyrus was highly useful as it was lightweight and took a negligible amount of space compared to the stone tablets. This allowed for more and more information to be preserved by writing it down on papyrus. This too continued for a long time and the Egyptian empire was one of the proponents and the largest users of papyrus. Over the years the papyrus went through various iterations and improvements to turn into the modern form that is called paper which is also an English word derived from the original papyrus. The invention of paper led to increased documentation and data preservation for a large number of books which are just the collections of large amounts of written paper.

A lot of individuals wrote groundbreaking books and have preserved that data in the form of books that safeguarded the information for the upcoming generation. But during this time, all of the books were handwritten. The process of making copies of books meant writing the whole book once again manually. This crept in a lot of errors and was a highly tedious process that took a long time and only a small set of books could ever be copied which decreased the potential of impact of such writings. This was the case up until the invention of the printing press. The printing press was an invention by Gutenberg, which was a revolutionary that forever changed the landscape of the planet.

The Gutenberg printing press could be used to produce numerous copies of a book that can be distributed. The increased number of books meant that the chances of survival were increased by a large margin. This also allowed for a much-optimized proliferation of knowledge which was earlier only accessible to the ultra-rich and the wealthy. Knowledge became affordable again and a plethora of users could take advantage of the situation and read books to enrich their knowledge. Books are one of the most efficient forms of data storage and this is the reason why they are still in widespread use in schools and other institutions.

But books have a limited amount of information that can be stored in them and the retrieval of such information from a large collection of books is highly difficult and a time-consuming process. This procedure was improved by the further invention of the computer or the computational machine and the various improvements that have been going on even today. The various alterations of the silicon wafer led to increasingly affordable and powerful computers that were capable of storing extensive amounts of information due to the introduction of the magnetic hard drive.

The hard drive has an extremely large storage space that can be utilized to store an exceedingly large number of books and there have been various tools designed that allow for the retrieval of the information from the various stored books very fast and efficient. This was further improved by the introduction of the internet paradigm. the internet paradigm was launched by the combination of computer researchers and the US military to design a system that connected the remote parts of the United States and allowed seamless communication between them. The Internet paradigm was also envisioned to allow researchers to remotely utilize the platform to allow remote access to various resources in the United States without traveling to a particular location.

After a few years, the internet was opened for public use and has been growing ever since the structure that encompasses the entire globe as the internet. This has allowed a large number of individuals and organizations to get connected to one another and allow for a much more seamless sharing of information and knowledge. The internet paradigm is also the birthplace of the cloud platform. The cloud platform utilizes the internet paradigm to allow for remote and pervasively available storage to the user anywhere in the world. therefore, this eliminates the costs associated with the purchase and maintenance of a local storage option and allows for a much more accessible cloud storage.

The cloud storage stores the information of the user or the organization on a remote server on the cloud platform. The user can, therefore, access his/her data from anywhere in the world with just an internet connection. The cloud platform is tasked with the maintenance and retrieval of the relevant data as when required which provides increased convenience for the user. Storage of one's sensitive and personal data on the cloud platform is highly dangerous as the remote server can get compromised the event of an attack. The compromised remote server can therefore, lead to a data leak scenario that can be highly detrimental to the user or the organization. Therefore, it is deemed as a safe practice to encrypt sensitive data before uploading it on the cloud platform for increased security.

The encryption techniques utilize cryptography to convert a normal plaintext data into a ciphertext, which resembles a collection of random characters and letters indistinguishable from its original format. Therefore, even if the remote server is compromised and the data stored on the server is leaked, the data of the user is safe as it is encrypted and the data is useless without decrypting it. Therefore, encryption is one of the most sensible choices when securing the data on the cloud platform. But there is a problem with encrypting the data as it makes it impossible to search and retrieve on the cloud platform. Storage of the private decryption key is not an option as it would be an unsafe practice.Section 2 of this research article represents the Survey on Past work done by the different researchers across the globe. In section 3 proposed techniques is being elaborated nicely to understand all technical deployment details. The Obtained results are evaluated in the section 4 and finally in section 5 this research article is concluded along with the future enhancement options.

II. Literature Review

H. Li explains that there has been significant growth in the internet paradigm as more and more users are utilizing this platform for the purpose of providing convenience for the users and the customers. The cloud platform is one of the most innovative concepts that has allowed the users to store their data remotely and access it anywhere in the world using an internet connection [1]. To safeguard the data on the cloud servers, it is in an encrypted format that is very difficult to perform the search. Therefore, the authors have proposed a Fine-Grained Multi-Keyword Search supporting classified sub dictionaries. The proposed technique has been demonstrated to be highly useful and accurate in the search metrics. The main limitation of the proposed technique is the lack of extensibility of the file set.

M. Ahmed states that in recent years there has been a visible growth in the number of internet users. This is due to the increase in the affordability of the platform which has made it highly accessible to the masses. Most internet usage has been attributed to the increase in the number of subscribers to the cloud platform as it allows for much easier access to their important data almost anywhere [2]. Due to security issues, the data is stored in the cloud is always encrypted which poses a great challenge for searching on the encrypted data. Therefore, the authors have proposed an effective dynamically indexed privacy-preserving multi phrase search on an encrypted cloud. The main limitation of the proposed technique is that the authors have not improved the index structure of the system.

H. Li introduces the utilization of the cloud computing platform for the purpose of storage and the retrieval of medical data. This paradigm allows the patient to keep track of their personal data which can be outsourced and authorized for the other medical professionals to refer the data stored for future reference. Encryption is a common technique that is used to provide protection of the data before uploading it to the cloud which makes it difficult to query and search [3]. Therefore, the authors have proposed an effective technique called SEDSSE or Secure and Efficient Dynamic searchable symmetric encryption which utilizes ABE or Attribute-Based Encryption and kNN or K Nearest Neighbor to achieve secure search on the cloud platform. The major drawback of this technique is that the authors have not released the assumptions.

L. Sun elaborates on the various different challenges faced by the cloud storage platform. The most threat to a storage system is through the attackers the want to gain unauthorized access to the user data which could lead to a data leak scenario. Therefore, to ameliorate this effect the authors in this paper have outlined an innovative technique for the prevention of insider keyword guessing attacks on a searchable public-key encrypted cloud storage [4]. The researchers have utilized indistinguishability obfuscation to achieve their goals and provide a secure and searchable public-key encryption technique. The main limitation of the proposed technique is increased computational complexity that is observed.

C. Guo explains that there has been a rise in the popularity of the cloud platform by a large amount recently. Cloud computing has been in increasing use in areas such as management flexibility and economic savings along with the management of personal data. The increasing amount of sensitive data needs to be secured through the use of encryption before uploading it on the cloud platform [5]. This practice makes it difficult o search over the encrypted data, therefore, the authors in this paper have implemented a dynamic multi-keyword ranked search based utilizing the bloom filter platform. The main limitation of the proposed methodology is the increased space complexity that is observed.

J. Preece addresses the issues that have been related to the security of the data that is being uploaded on the remote servers in a cloud platform. The cloud platform has been increasingly used for the storage of large amounts of data which includes the large industrial data that is being uploaded on this framework which is highly sensitive in nature. Therefore, the authors have proposed an efficient and secure technique for encryption of the industrial data on the public cloud infrastructure [6]. The proposed technique has been demonstrated to achieve acceptable security for the stored data. The main drawback of the proposed technique is that the computation of the symmetric keys that have not been shifted to a distributed context.

W. Shen states that the cloud platform has been highly utilized for the purpose of storage nowadays. An increasing number of users and organizations have been adopting this framework to provide efficient and seamless management of their data. This includes the EHRs or Electronic Health Records that contain sensitive and personal data of the patients. Therefore, to secure the data the authors have proposed an efficient identity-based integrity auditing and data sharing while hiding sensitive information on cloud storage. The proposed technique has been evaluated to provide efficient security and also secure sensitive data [7]. The major drawback of the proposed technique is the increased computational complexity that is observed.

Y. Zhang introduces the concept of cloud-based storage that allows the users to upload their data on to a remote server to be able to access it anywhere in the world through the use of the internet. This allows for the data to be available to the user at any given time rather than relying on local storage options that are not portable. This also increases the risk of the data being under attack or in a data leak scenario. Therefore, to secure the cloud storage systems the authors have presented and efficient technique for the verification of the data integrity as well as the protection of the system from indistinguishability obfuscation. The presented technique has been demonstrated to perform satisfactorily [8]. The main limitation of the proposed technique is that the authors have not balanced the performance on the cloud as well as the client which causes additional overhead.

W. Shen addresses that there has been an increase in the number of users that have been reducing the expenditure on the local storage options and are rather opting for utilizing cloud storage systems that have been known to be maintenance-free. To secure the data on such cloud storage systems that often store user data on remote data servers, encryption is utilized and a private key is generated for its use, most auditing systems utilize this private key for auditing purposes that can be an area of weakness for an attack [9]. Therefore, the authors have proposed an efficient and secure data integrity auditing scheme that does not utilize the private key for secure cloud storage. The main limitation of the proposed technique is that there is a time complexity observed in the proposed methodology.

M. Yadav states that there has been a rise in the popularity of various different cloud services. This is due to the fact that the cloud framework allows for an increased convenience that is not being offered by the local storage prices as well as the maintenance costs that if offers. The cloud also has an added advantage of being accessible anywhere in the world with an internet connection [10]. Therefore, the authors have proposed an efficient keyword search technique on the cloud platform that utilizes Fuzzy Logic to achieve its performance. The proposed technique has been experimented on to ascertain its performance which has been up to the mark the main limitation of the proposed technique is the slow speed of the querying engine.

J. Duan explains that there have been many integrity assessment techniques that have been focused on improving the performance of the integrity assessment. It is also known as the integrity auditing mechanism is the most vulnerable part of cloud storage services as it can allow an attacker to gain unauthorized access to the data. therefore, the authors in this paper have proposed an integrity attack on a consensus-based energy management algorithm [11]. The proposed attacks are performed in a simulation environment with immense success. The Future Renewable Electric Energy Delivery and Management or FREEDM system is a part of the proposed methodology.

Y. Yu elaborates on the practice of remotely monitoring and performing maintenance on a server through the use of integrity evaluation techniques. There have been numerous instances of the integrity auditing system being hijacked and used by malicious users and attackers which gain access to the encrypted cloud very easily [12]. This is the reason why the integrity evaluation system on a cloud server needs to be safeguarded with the utmost scrutiny this is the reason why the authors have proposed a Data integrity checking remotely using identity-based privacy-preserving cloud storage. the experimental results prove the superiority of the proposed technique.

K. Pavlou states that there has been an increase in the incidences of database tampering that has been done using unauthorized access by the attackers for the fulfillment of their nefarious agendas. Once the database has tampered with it can leave some trace of evidence of the attacker’s identification that needs to be analyzed forensically to determine a result [13]. Therefore, the authors in this paper have proposed an efficient tiled bitmap forensic analysis algorithm as an optimal algorithm that identifies the possible locations of the tampering and complete characterization of the datasets cardinality that allows for an accurate assessment of the crime committed by the attacker.

P. Sreekumari examines the popularity of the big data platform that has been utilized with increasing frequency nowadays. It has been attracting significant amounts of attention from the media, the industry and the academic organizations all over the world. A large number of organizations have been utilizing this platform for searching, analyzing, processing and storing their data [14]. This type of usage exposes sensitive data to attacks that can lead to data leakage which would give significant amounts of damage to the organization. Therefore, the authors in this publication perform an extensive analysis of the keyword search schemes that preserve privacy on an encrypted cloud platform.

Y. Zhang explains that there has been a significant amount of increase in the number of organizations and individuals that are adopting the cloud framework for the purpose of outsourcing their data. A lot of users have been shifting their reliance from the local storage to the cloud storage due to the increased convenience and the decreased security is the main concern. Therefore, the authors in this paper have proposed a keyword search technique on a blockchain assisted public key encryption-based cloud storage against the keyword guessing attacks that are popularly performed on the cloud storage facilities. The experimentation results indicate the proposed methodology has been performing as expected [15]. The main drawback of the proposed technique is that the authors have not enhanced the functionality, efficiency, and security of the data outsourcing systems.

III. PROPOSED ALGORITHM

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

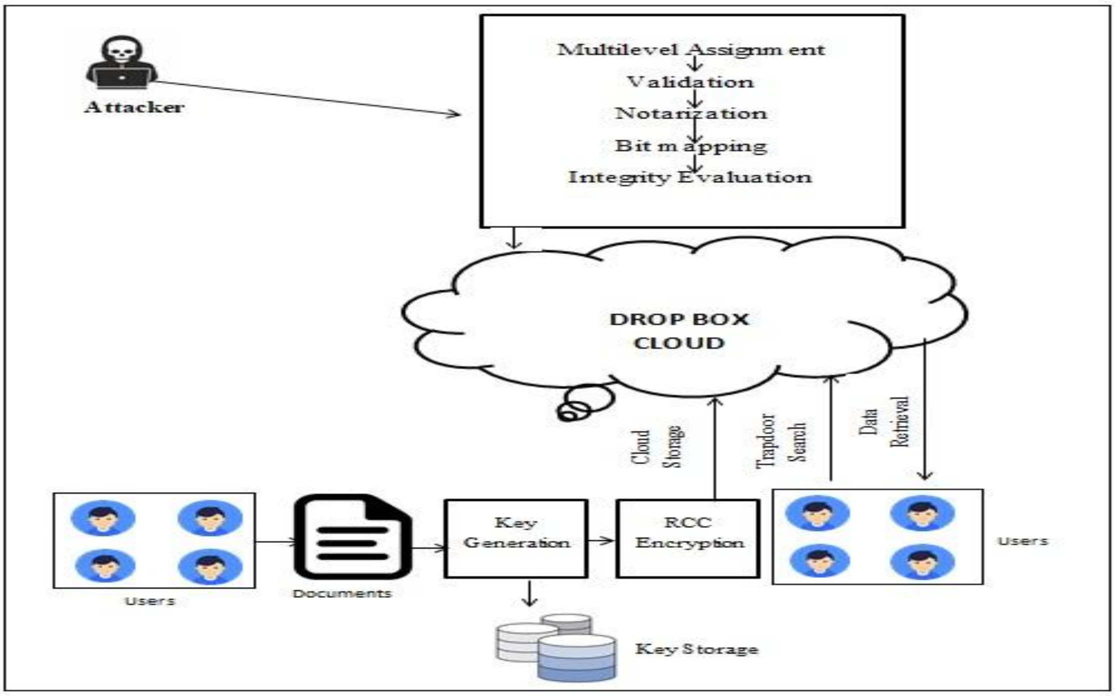


Figure 1: Overview of the proposed model

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  $M_{HK}$
//Output: Key
Start
KEY =” ”
IND= $M_{HK}$ length MOD 7
    FOR i=0 to KEY Length <7
        i=i+( IND +1)
            IF ( i< $M_{HK}$ length)
            KEY=KEY+ $M_{HK[i]}$
            $M_{HK}$ = $M_{KH}$ >> 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.

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: Search Over Encrypted Data:

As the file is being uploaded to the cloud its features are being extracted and they also stored along with the original file. Once user is fired a query to search a file which is in the encrypted format, then Query String from the user is subjected to preprocessing. By doing this the string is getting rid of the unwanted text that really does not add any meaning to the text and also it makes the string more lightweight, which will be the added advantage to reduce the complexity of the process. Before performing the preprocessing step, the single document string is split on "." Character to retrieve the sentences and then these sentences are stored in a list. The preprocessing includes the four steps as mentioned below.

Special Symbol Removal - Here in this step all the special characters from the strings are shred off except the space character and ".".

Tokenization- Here special symbol removed string is split on the "." to get the string into a list. Then each of this string is subjected to Stopword removal and Stemming process.

Stopword Removal- This is the step of removing all the conjunction words from the sentences like and, of, the, from, to etc. By removing these words, the semantics of the string remains intact.

Stemming -Stemming technique brings down any word to its base form and this makes the word lighter in weight and meaning of the word remains unchanged.
This preprocessed string is tokenized to create a bucket of sub word list. This bucket is then encrypted to get the indexed list for searching to call it as Trap door. This trap door is labeled to search the files that are stored in the cloud using the similarity measure to retrieve the desired files.

Step 4: Data Integrity:
This module designed to evaluate the integrity of the stored files in the cloud using the Bit mapping technique. In this module each and every document are being visited in the set interval of the validation time. At each interval of the time the notarized hash key is being fetched and stored in the bitmap array to compare with the next iteration bitmap array. On any dissimilarity between the bitmap array, hash key smells the integrity violation of the array to generate the desired report. This whole process is conducted in parallel computed by dividing the number documents to load in in individual threads in the step of multilevel assignment.
The whole proposed system is expressed mathematically with the below model.

Mathematical Model

1. S= {} be as system for Enabling Search Over Encrypted data and Data Integrity Evaluation in Cloud
2. Identify Input as D= $\{D_1, D_2, D_3 \ldots\ldots D_n\}$
Where D= Document
S= {D}
3. Identify R as Output i.e. Retrieved Files.
S= {D, R}
4. Identify Process P
S= {D, P, R}
5. P= $\{K_G, D_E, P_R, S_E, D_I\}$
Where
K_G =Key Generation
D_E = Document Encryption
P_R = Preprocessing
S_E = Search over Encrypted Data
D_I = Data Integrity

6. So the Complete system for search over encrypted data and Data integrity can be given as

S = $\{D, K_G, D_E, P_R, S_E, D_I, R\}$.

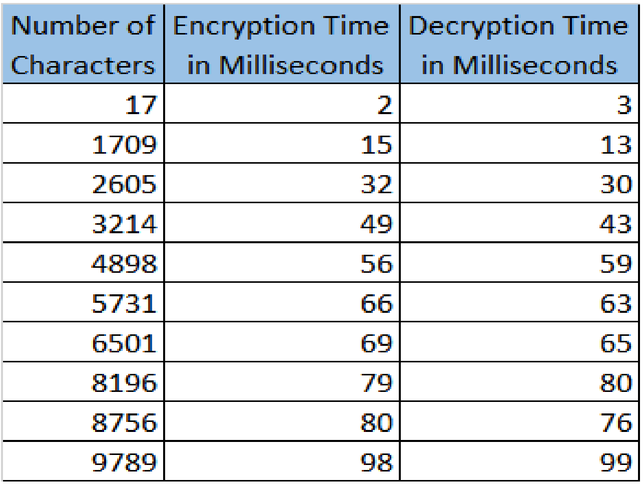
IV. Result And Discussion

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.

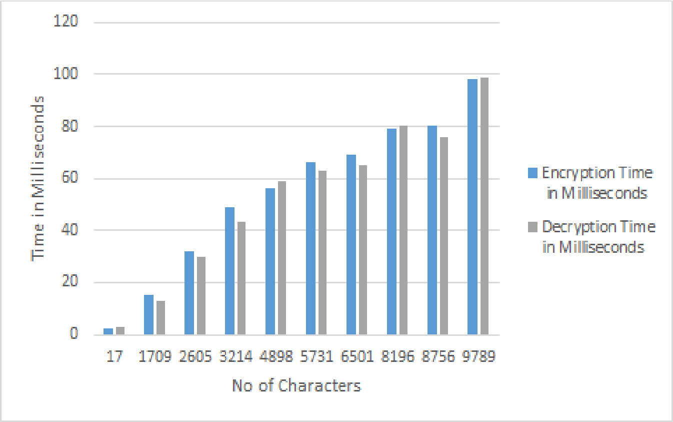
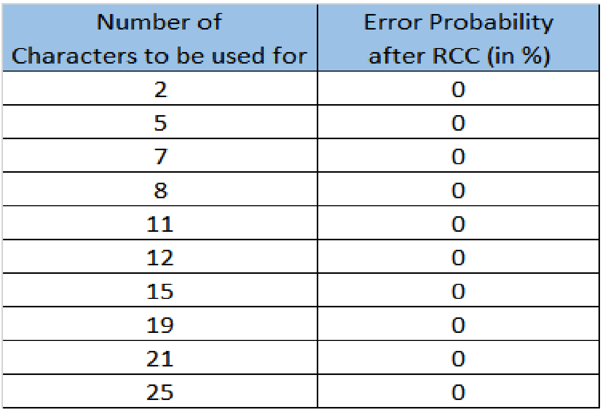


Figure 2: Encryption and Decryption Time

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

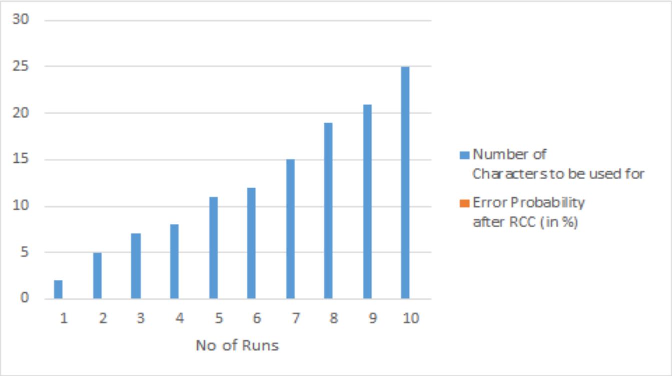
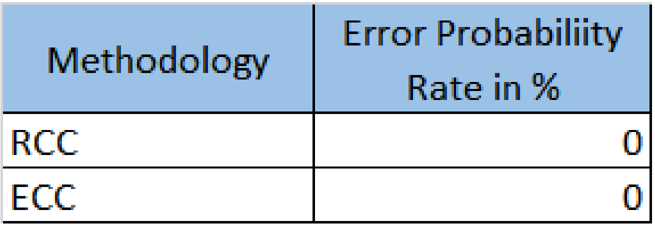


Figure 3: Error probability after message Decoding using RCC reading



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 [16], 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 cloud security mechanism is detailed in this paper that utilizes the Reverse Circle Cipher along with the usage of tiled bitmap algorithm for providing an effective Security for the data. The proposed system also uses search over encrypted data mechanism to fasten the process of searching. 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. H. Li et al, "Enabling Fine-grained Multi-Keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, 2016.
2. M. Ahmed et al, "Privacy-Preserving Dynamically Indexed Multi-Phrase Search over Encrypted Data", International Conference on Advances in Computing, Communications, and Informatics (ICACCI), 2018.
3. H. Li, Y. Yang et al, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data", IEEE Transactions on Cloud Computing, 2017.
4. L. Sun et al, "Secure searchable public-key encryption against insider keyword guessing attacks from indistinguishability obfuscation", Science China Information Sciences, 2018.
5. C. Guo et al, "Dynamic Multi-Keyword Ranked Search Based on Bloom Filter Over Encrypted Cloud Data", IEEE Access, 2019.
6. J. D. Preece and J. M. Easton, "Towards Encrypting Industrial Data on Public Distributed Networks", 2018 IEEE International Conference on Big Data (Big Data), IEEE, 24 January 2019.
7. W. Shen et al, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, VOL., NO., 2018.
8. Y. Zhang et al, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation", IEEE Transactions on Information Forensics and Security, 2016.
9. W. Shen et al, "Data Integrity Auditing without Private Key Storage for Secure Cloud Storage", IEEE Transactions on Cloud Computing, Vol., No., 2018
10. M. Yadav et al, "Encrypted Keyword Search in Cloud Computing using Fuzzy Logic", 1st International Conference on Innovations in Information and Communication Technology (ICIICT), 2019
11. J. Duan et al, "A Novel Data Integrity Attack on Consensus-based Distributed Energy Management Algorithm using Local Information", IEEE Transactions on Industrial Informatics, 2018.
12. Y. Yu et al, "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information Forensics And Security, VOL. 12, NO. 4, April 2017
13. R. Snodgrass et al, "The Tiled Bitmap Forensic Analysis Algorithm", IEEE Transactions on Knowledge and Data Engineering, Vol. 22, No. 4, April 2010.
14. P. Sreekumari, "Privacy-Preserving Keyword Search Schemes over Encrypted Cloud Data: An Extensive Analysis", 4th IEEE International Conference on Big Data Security on Cloud, 2018.
15. Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, and Xuemin Sherman Shen, "Blockchain-Assisted Public-Key Encryption With Keyword Search Against Keyword Guessing Attacks For Cloud Storage", IEEE Transactions on Cloud Computing (Early Access), IEEE, 17 June 2019.
16. 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details