WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Research on Privacy Preserving using Attribute Based Encryption Technique in Cloud Computing

[1]Pankaj Shukla, [2]Pankaj Richhariya

[1,2]Department of Computer Science & Engineering, Bhopal Institute of Technology & Science, Bhopal
[1]pankaj26jn@gmail.com

ABSTRACT

The global spread of cloud computing technologies has revolutionised the internet. The cloud's virtual platform, infrastructure, and software utilisation has created a setting in which the user may store and utilise the programme from any location. This has made people consider the security of data stored in the cloud. This work discusses attribute-based keyword search over encrypted data in the cloud, which offers security over keyword-based data searching. The cloud now offers real-time and crucial applications that are part of next-generation computing. Flexibility, scalability, and fine-grained access control are the primary components. This is only possible in a classical architecture when the user and server are in a trusted domain. ABE's encryption is simple, secure, and reasonably priced when compared to other encryption. Because the qualities rather than the contents are included in the encrypted data, the ABE is secure. The programme is safe thanks to attribute-based encryption. ABE performs well when compared to other encryption techniques. As a result, attribute-based encryption will be the future of all cloud apps. In ABE, encryption is carried out using a one-many technique, which implies that it is done for a larger group of users rather than just one. So, this approach of defining a control system was not more expressive. To preserve the authentication and security of the data, modifications made to policies are implemented in encryption mechanisms.

Keywords: *Cryptography, Cloud Computing, Attribute Based Keyword Search.*

Introduction

Cloud Computing lets users access a variety of resources and services as needed. Because the user is given access to a variety of internet-based services, he need only pay for the ones that he wants to utilize. In cloud computing, users can access any service they choose from a common pool of services. The user's data, however, is stored on a cloud server in cloud computing. This is risky and needs an effective handling mechanism to maintain the data's integrity. In order to provide safe cloud storage for the users' data, several academics have developed a number of ways. These mechanisms employ different cryptography-based strategies to provide secure cloud storage for the users' data. Schemes like ABE (Attribute Based Encryption) are used to provide a secure storage for the clouds data.

In cloud a large amount of data is stored which contains confidential information. Data like PHR (personal health records) is generally stored at third party environment which contains confidential concerns, thus a secure handling for that data is required, and a secure cloud storage technique for the PHR data is presented in this dissertation which provides an enhanced functionality to the user's data.

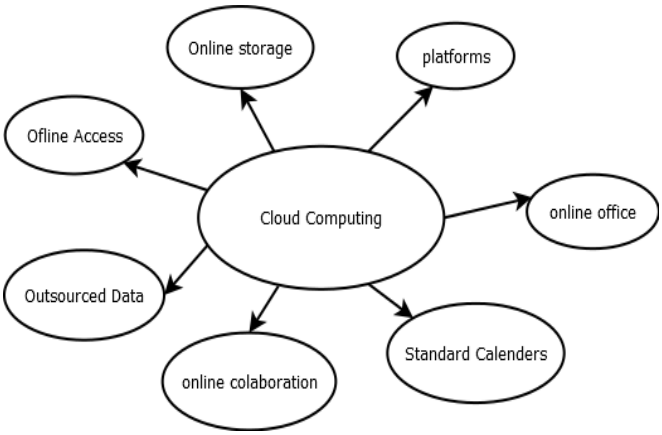

Figure 1: Overview of Cloud Computing.

Cloud computing is the process of storing and accessing data and software through the Internet as opposed to your computer's hard disc. The Internet may be compared to a cloud. It dates back to the time when presentations and flowcharts would depict the vast server-farm architecture of the Internet as nothing more than a fluffy, white cumulonimbus cloud that was accepting connections and dispersing data as it floated.

The idea of cloud computing is not new. In one way or another, we have been utilising cloud computing for a very long time. Simply put, you may think of the cloud as a very large server that is home to a variety of services and data that you can use for professional purposes. The applications and data that you use for work are stored on the server, not on your machine. Cloud Computing is the idea of using services that are not stored on your computer.

1.1 Attribute Based Encryption

Public key cryptography is a modern strategy that is used in attribute-based encryption (ABE). A communication is encrypted using the individual recipient's public key in public key cryptography. By treating the public key as a string and the identities of the recipients, such as their email addresses, identity based cryptography or identity based encryption is used to encrypt data. ABE provide and enhanced way of the encryption, a set of the attribute of the receiver is used to encrypt the message for the receiver. In KP-ABE (Key policy Attribute Based Encryption), policies define over the attributes are used to perform encryption or encrypt message. In that technique a person can be able to decrypt the message only if he can have the matching key to decrypt the message. That way it provides an enhanced security mechanism for the user.

1.1.1 Cipher-Text Policy ABE

A user's private key is linked to a collection of attributes in cipher-text-policy attribute-based encryption (CP-ABE), and a cipher-text provides an access policy over a set of specified attributes inside the system. If and only if a user's characteristics match the cipher-text's policy, that user will be allowed to decode the given cipher-text. There are structures for regulations referred to as arbitrary circuits as well as ways to define policies over attributes using conjunctions, disjunctions, and (k, n) (k, n)-threshold gates, where k out of n attributes must exist. There are additionally non-monotone access rules with extra negations. For instance, let us assume that the universe of attributes is defined to be {A,B,C,D}{A,B,C,D} and user 1 receives a key to attributes {A,B}{A,B} and user 2 to attribute {D}{D}. If a cipher-text is encrypted with respect to the policy (A∧C) ∨D(A∧C)∨D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.

Thus, CP-ABE enables the realisation of implicit authorisation, whereby the permission is built into the encrypted data and only those who adhere to the corresponding policy may decode the data. Users may retrieve their private keys once data has been encrypted in accordance with rules, which is another excellent feature. Therefore, data may be encrypted without knowing the precise group of users who will be able to decode it; instead, just the policy that permits decryption is specified. Any future users who are provided with a key with regard to the qualities necessary to satisfy the policy will thereafter be able to decrypt the data.

1.1.2 Key Policy ABE

KP-ABE is the d9ual to CP-ABE in the sense that an access policy is encoded into the users secret key, e.g., (A∧C)∨D(A∧C)∨D, and a cipher-text is computed with respect to a set of attributes, e.g., {A,B}{A,B}. In this example the user would not be able to decrypt the cipher-text but would for instance be able to decrypt a cipher-text with respect to {A, C} {A, C}.

Collusion resistance is a crucial characteristic that both CP- and KP-ABE must attain. This essentially implies that it should not be feasible for different users to "pool" their secret keys in order to jointly decode cipher-text that neither of them could separately decipher. This is accomplished by independently randomizing users' secret keys, which is what is meant by this statement.

A kind of public-key encryption known as attribute-based encryption is one in which a user's secret key and the cypher text are determined by attributes (such as the nation in which he resides or the type of subscription he has). In such a system, a cipher-text can only be decrypted if the user key's set of characteristics coincides with those of the cipher-text. Collusion-resistance is a key component of Attribute-Based Encryption's security: Only if at least one specific key allows access should an enemy with numerous keys be allowed to access data.

2. Literature Review

Private well-being document (PHR) is in most cases noticeable as a patient-pushed model of sharing well being related expertise. But protection is the prime concern while storing data in an outsourced atmosphere. If the full entry of the PHR information is supplied to the patients that simply waste for him to preserving that knowledge. However there are disorders like dangers of the security introduction scalability in the key management and many others are the difficulties in delivering a nice-grained service to the consumer and provide a cryptographically approved provider. Patient data is encrypted using an ABE (Attribute founded Encryption) service to give a fine-grained and comfortable access control. In this way, not only a security mechanism but also a fine-grained carrier and a division of the patient's data into several security domains are given. That reduces the complexity in the administration. A cozy framework to share sufferers' information over the outsourcing environment is furnished, that helps to share patient's PHR knowledge over the internet, which can be used within the therapy of the various ailments. A comfortable world access is furnished to the opposite users like doctors to uses this data for the remedy of the illnesses [1].

Personal wellness report (PHR) is sufferer pushed model of individual wellbeing records sharing, which is commonly outsourced and put into the 0.33 occasion server, for example, cloud provider. There is among the biggest safety considerations, in view that personal health documents are saved in 1/3 occasion server in the untrusted atmosphere. Consequently there may be various cryptography strategies can be used to encrypt that information before outsourcing it. Patients now have control over who has access to their information thanks to this. A patient-driven model and an entry control framework are used to prevent unauthorised access to PHR data. An Attribute based encryption process and a One Time Password (OTP) centered technique is used to furnish better performance to relaxed outsourcing of the information. Dynamic entry manipulate framework is provided to the patient for secure outsourcing to their knowledge [2].

Japan is likely one of the countries where way forward for nation is probably the most raised in the world. Not handiest bettering the social medication services but additionally improving in social wellbeing care protection framework, person actions within the social services and many others. Thus PHR (individual wellness record) of the every sufferer can be used to provide expertise about the diseases which used to medication or in treatment of those ailments. Wellness knowledge evaluation is performed to furnish higher information in regards to the health care data. That digital health care data can be used through the general population to and the medical authorities to fortify the wellness care offerings. But when put that knowledge available to the general population can be cause serious protection difficulty for the patients personal data. A appropriate administration and management is required to furnish a secure entry for that information [4].

As a rising patient-driven mannequin of wellness information sharing, cloud-centered individual health file (PHR) framework holds top notch assurance for enticing patients and guaranteeing more compelling conveyance of medicinal offerings. A novel sufferer-driven cloud-based comfy PHR framework, which allows patients to soundly retailer their PHR information on the 1/3 get together cloud server, and above all share their PHR information to an broad form of customers, together with medical services supplier like doctors and attendants, loved ones or companions. To cut back the important thing administration multifaceted nature for doctors and purchasers, we partition the customers within the cloud-based PHR framework into two safety areas named open space and individual area. Instead of using the previous Cloud-based PHR framework, PHR owners now scramble their PHR data for public spaces using a definite content procedure property-based encryption plan, while they encode their PHR data for private spaces using a mysterious multi-recipient personality-based encryption plan. Simply approved purchasers whose qualifications fulfill the predefined figure content material procedure or whose personalities fit in with committed characters can decode the encoded PHR understanding, where figure content material association or committed personalities are inserted within the scrambled PHR understanding. The patient-driven cloud-based pleasant PHR architecture is demonstrated through extensive investigative and exploratory outcomes to be comfortable, adaptable, and productive [5].

Individual well-being records (PHRs) have to stay the lengthy lasting property of sufferers and must be showable to the licensed customers or like doctors and different healthcare authorities. In present situation PHR makes a speciality of the ordinary information sharing corporations and provide international healthcare framework. My PHR computing device, a sufferer- pushed mannequin is provided, that presents a more desirable framework wellbeing records sharing. In that procedure not most effective the scientific understanding but in addition related expertise to that programming of PHR is also shared. In that procedure knowledge shared over the cloud which can be utilized with the aid of the various customers. Patients can utilize a remote virtual desktop to obtain the information. The patients, medical professionals, insurance companies, and many other groups are given access to comprehensive PHR information. to obtain effective treatments for the disorders [6].

Personal wellness documents (PHRs) are methodology to make patient centric health offerings. There's some work is required to furnish better wellness care offerings to the patients at house and difficulties in work procedure like have an effect on of the access of these records, psychological influence, physical have an impact on etc. The results of these healthy evaluation is used by the quite a lot of companies to furnish better health care offerings to the sufferers. That help in growth of the healthcare offerings and get to the bottom of the issues of the sufferers related to the well-being care services [7].

To recognize the difficulties barriers happened with delivering individual wellbeing files (PHR) to the patients and corporations is presented. A gain knowledge of over the PHR and well-being services in last decade is performed. In that evaluation is carried out for the technological know-how acceptance mannequin in PHR sharing. Protection is likely one of the greatest predicament in cloud computing which require evolved dealing with for such drawback. There are more than a few procedure offered by using the researchers to furnish cozy information sharing over the cloud. There are well-being care carrier supplies which tailored that model and participate in the venture to share digital healthcare knowledge over the cloud which helps the healthcare service providers to make policies for the consumer [8].

This work suggested a piece TPA effectively conducted batch auditing support, enabling several files to be audited without access to the tpa or cloud. This allowed TPA to engage in audits for multiple users at once. A thorough examination of protection and effectiveness reveals that the suggested systems are demonstrably safe and highly effective. They have implemented features that enable an external auditor to audit a customer's cloud data without knowing the data's contents, allow the TPA to manage multiple concurrent auditing tasks from different users while maintaining privacy, implement a MAC-based setup, and use a hashing algorithm to participate in auditing while handling the data. The experimental setup and findings were conducted out using the existing ECC and MAC system. Results and efficiency assessments have been made for a number of features, including taking some sample blocks and computing a number of effect factors, including server computation time, cloud computation time, and verbal exchange cost. This scheme uses the holomorphic linear authenticator and random covering to ensure that the TPA won't learn anything about the information content stored on the cloud server for the duration of the effective auditing process, which not only frees the cloud user from the time-consuming and likely expensive auditing task but also allays the customers' fear of their outsourced information [9].

Advanced Encryption Standard, or AES, was created by NIST in 2001. The public key technique known as RSA was developed in 1978 with the assistance of Rivest, Shamir, and Adleman. It is also referred to as the uneven key method since it uses different keys for encryption and decryption operations. Each algorithm has unique fundamental object sizes that set them apart from one another. 56 bits make up the DES algorithm's primary factor measurement. The AES algorithm uses a key size of 128, 192, and 256 bits. The Blowfish algorithm's primary thing dimension is 128–448 bits. The RSA algorithm's primary factor dimension is 1024 bits. Consequently, the writers of this article used a number of methods, and they compared the results to the total number of algorithms [10].

3. Problem Description

The following related issues in the current system are addressed in our suggested work:

• If AES-256 were to ever fail, it would be quite easy for hackers to exploit.

• The current accessing and storing system requires a lot of processing time.

• As a result, data storage is expensive while still allowing for access.

• For suitable loose coupling, the currently extended algorithm usage model is needed.

• The previous method had a restriction on obtaining data from huge dataset structures.

• The base article does not include highly indexed data structures, which requires further examination of high end access.

4. Proposed Algorithm

In order to computer the enhanced work from the study of previous algorithm here a proposed algorithm name EECC algorithm is proposed by us which is efficient while comparing with the existing ECC and MAC algorithm for the encryption and data storage security.

- The proposed work can be done in accordance of working with security and storage over the various available component . data optimization over the network and to work on reducing better resource management and CRM investigation can be done in further proposed methodology.
- An advance accessing mechanism with process security is going to process in proposed approach with lexical storage and HECC security approach.
- The above algorithm pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here.

4.1 Advantage of Proposed Algorithm

The proposed security method will be utilised in conjunction with the system for storing and accessing lexical data.

• Data that is resource conscious and pre-computed will aid in quick calculation and decision-making.

• Low calculation time and high throughput will be seen.

• Improvements in encryption technology utilise algorithms to facilitate effective data exchange.

• The run-time execution and the present execution will be saved by a simultaneous dynamic search update.

The proposed scenario is shown in its entirety in the image below, which accurately depicts our work and computes the parameters.

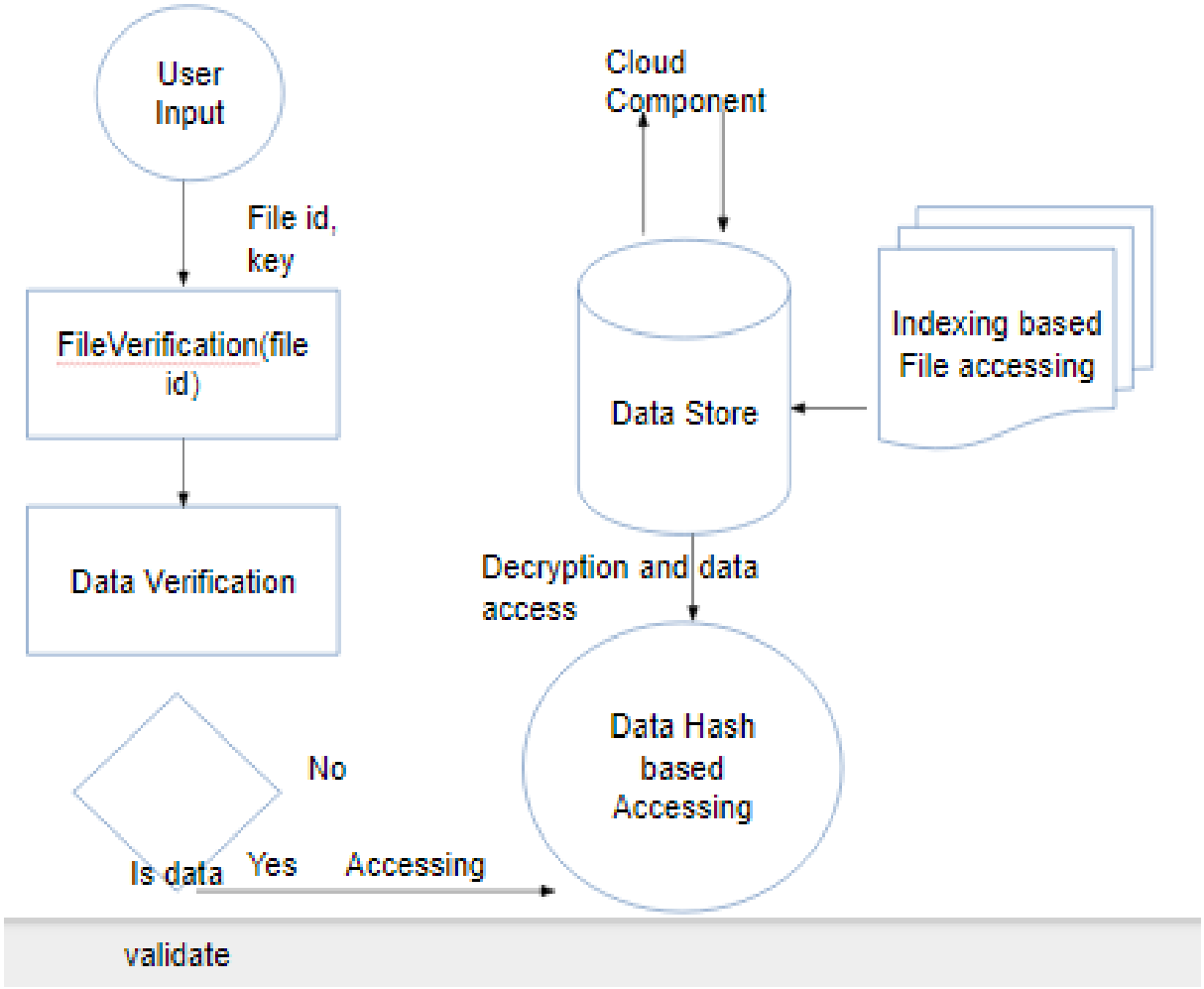

Figure -1: Storage & Access End Flow Diagram.

The complete process is divided into sub module which are taking part to complete the process, such as key generation, hash tag generation, file data encryption , further the encrypted data to store into the cloud data center, requesting for the file tag and integrity proof and finally user gets the output in the safe or unsafe mode.

KeyGen(File ID , File Data, Input) – HECC data key generation to perform the encryption over algorithm is going to perform using this present scenario.

This is the module where the key generation occurred among the available given input scenario. Here the detail accessing and input strategy is going to observe such that efficient key for the algorithm input can generated.

TagIndexHashGen(FileData) – The module contains the process of generating lexical hash indexing such that the process in process storage and accessing can be perform using the algorithm .

EncFile(FileData, Key)- ECC extension that's HECC which is hyper version of ECC algorithm is going to perform in this phase.

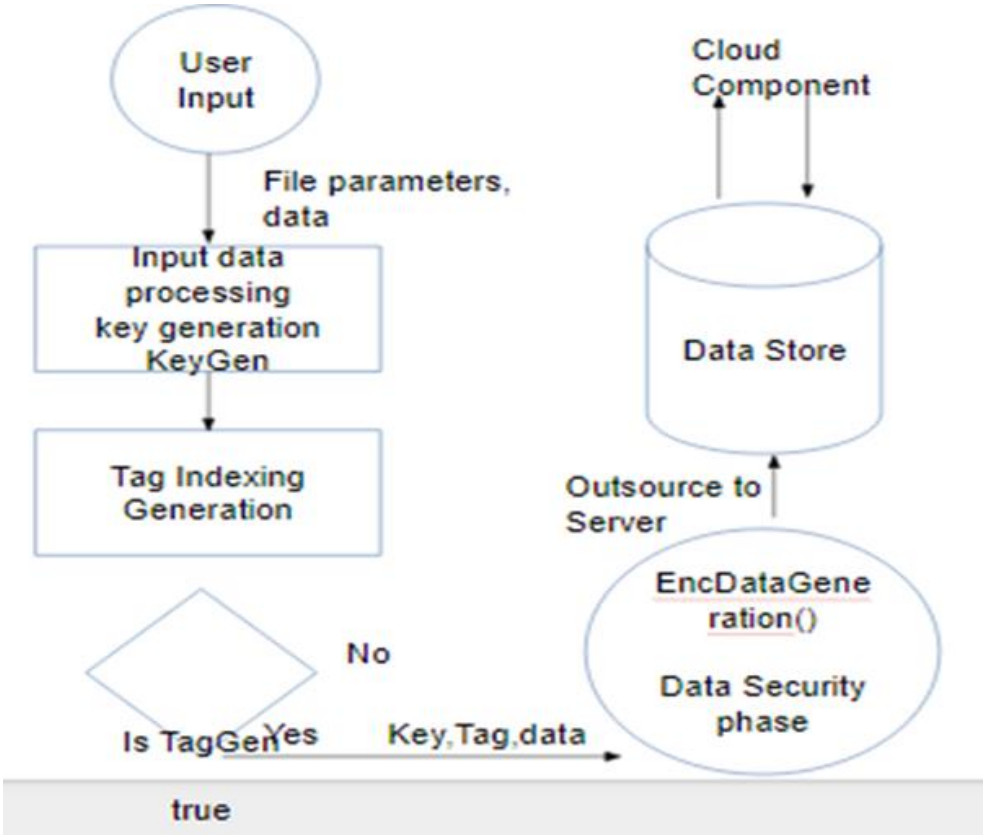

Figure 2: Accessing End Flow Diagram.

FileUpload(EncFile,key) – Data storage in lexical format is working in this module, thus the upload can be store and work at searching module.

verifyDataRequest(FileID)- In this module data verification , assignment , accessing role, permission is going to perform.

TPA End Algorithms:

DataVerification(FileID, input) – Data accessing and genuinity verification occurs in this module of cloud.

ProofGenerator()- this module is also designed at TPA end to provide a file safety proof where the proof claims the data safe or unsafe at data center cloud end.

Cloud Service Provider: DataLexStore(EncData)- Data storage for the file is perform in lexical manner.

5 Simulation Requirement

A piece of hardware or software that simulates network behaviour does so without actually displaying a network. Cloud simulation is a method used in cloud computing research that analyses how different cloud computing devices interact with one another or by using mathematical formulae. Simulators mimic clouds with a variety of devices, linkages, and applications, which are then examined to gauge their performance. The cloud simulators may also be customised by users to meet their own analysis needs. The criteria for simulation [12] in cloud computing are as follows:-

A. Cloud Simulator (For Cloud Simulation, We Used The CloudSim API & Apache Server)

B. Jdk or NetBeans Development Environment

C. Database

5.1 Cloud Simulators

Cloud simulators are the simulators used in the cloud computing simulation process. Because cloud computing is a new and rapidly expanding technology, several cloud simulators have been released, however many have extremely subpar libraries, packages, and methodologies. The following is a list of some cloud simulators that may be used to gauge cloud computing: -

1. CloudSim

2. iCanCloud

3. CloudAnalyst

4. GreenCloud

5. VirtualCloud

-

5.2 CloudSim:A Framework for Modeling and Simulation

The most effective method for providing scalable, fault-tolerant, safe, and dependable services for computation is cloud computing. Prior to the actual production of cloud products, new cloud applications and policies must be evaluated using timely, repeatable, and controlled procedures in order to guarantee the presence of such qualities in cloud systems under development. The use of simulation is possible since using real test beds restricts the experiments to the size of the test bed and makes it extremely hard to replicate the results. The purpose of CloudSim is to offer a generalised and extensible simulation framework that enables modelling, simulation, and experimentation of developing Cloud computing infrastructures and application services. This allows its users to concentrate on particular system design issues they wish to research without having to worry about the nitty-gritty specifics of Cloud-based infrastructures and services.

5.3 Simulation Parameters

5.3.1 Computation time

The amount of time needed to complete a computing operation is called the computation time. A series of time slots for executing computations on the various services' accessible segments can be used to represent calculation time. The amount of services has an impact on the computation time.

6. Result Analysis

Given the system's requirements and how we developed them, a comparison study based on factors such key size, server computation time, and TPA computation time was conducted, and the results showed that our suggested scenario was the best method at our disposal.

Table 1: comparison computation between existing and proposed computation time at server end.

Algorithm Name/ Data Size	Existing ECC (Server End)	Enhance ECC (Server End)
5 MB	5654 ms	5600 ms
10 MB	4555 ms	4500 ms
15 MB	11890 ms	11800 ms

Table 2: comparison computation between existing and proposed computation time at TPA end.

Algorithm Name/ Data Size	Existing ECC (TPA End)	Enhance ECC (TPA End)
5 MB	2311 ms	2300 ms
10 MB	1980 ms	1900 ms
15 MB	7123 ms	7100 ms

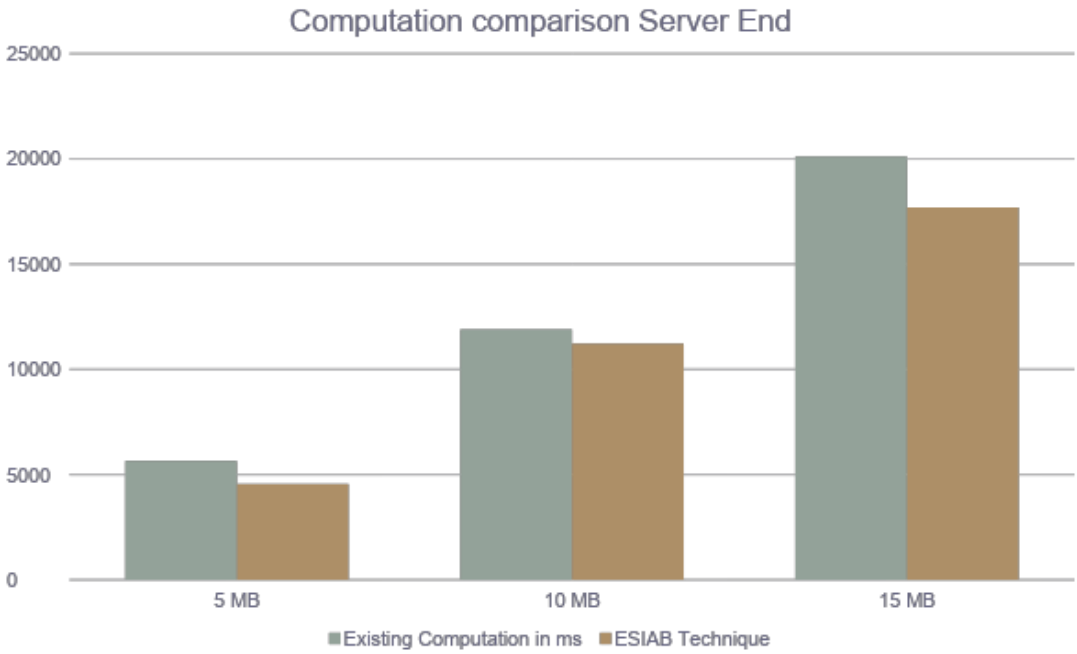

Figure 3: Bar graph comparison analysis in between implemented algorithm server side.

The above figure which represents the comparison analysis part in between the Existing ECC based encryption algorithm and the proposed ECC being proposed in our implemented work, the graph shows the efficiency while working at server side.

The computation time while transferring data or uploading the data to the cloud server it make efficient computation compared with the existing ECC algorithm.

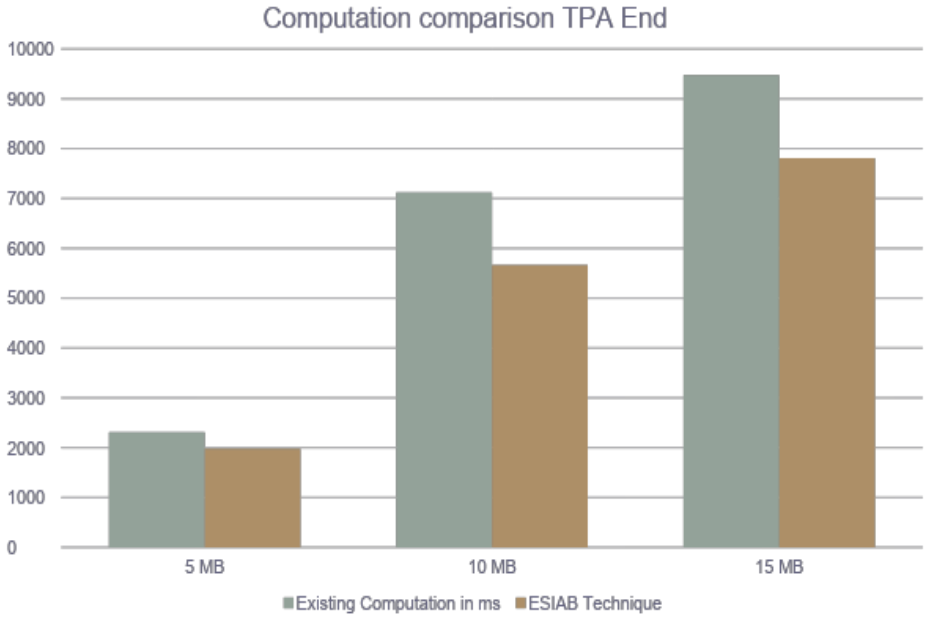

Figure 4: Bar graph comparison analysis in between implemented algorithm TPA side.

The figure above demonstrate the computation time which is being taken while communication performed by the TPA, the operation such as data integrity verification and correctness of data computation data is performed at TPA side , the result comparison given high performance which is shown in above bar graph.

7. Conclusion

As per discussed and algorithm performed by us in the area of cloud commutating. The considered work from the traditional algorithm taken as ECC and MAC for the encryption purpose and the key exchange and data distribution among the range of data. The proposed work performed by us is enhancing

ECC where the SHA-2 takes part for the key generation and hash tag generation process. Our work also simplify the modules take part in complete process and finally the data is stored in encrypted form and hash tag for the same file id stored, further the integrity verification and proof generation is performed by us. The proposed work is conducted at configured cloud server accessed from remote location using static IP driven. The result we computed using the computation time and key exchange system given by the proposed system outperform better in proposed work.

As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

8. Future Work

As per discussion the proposed algorithm outperforms best in its field where both the encryption and hashing perform best among. Our further work will be implementing the system and algorithm with multiple authority system and also to perform them in parallel to get our result in heavy traffic cloud environment.

References

1. Parvatikar, S., Prakash, P., Prakash, R., Dhawale, P., & Jadhav, S. B. (2013). Secure sharing of personal health records using multi authority attribute based encryption in Cloud Computing. *International Journal of Recent Advances in Engineering\& Technology (IJRAET)*, *5*, 50-52.
2. Konda, S., & Reddy, N. (2013). Enhanced Scalable and Secured Sharing of Personal Health Records in Cloud Computing Based on Attribute Based Encryption with Integrity Proof. *International Journal*, *3*(9).
3. Price, M., Bellwood, P., Kitson, N., Davies, I., Weber, J., & Lau, F. (2015). Conditions potentially sensitive to a personal health record (PHR) intervention, a systematic review. *BMC medical informatics and decision making*, *15*(1), 1-12.
4. Sutanto, J. H., & Seldon, H. L. (2011, September). Translation between HL7 v2. 5 and CCR message formats (For communication between hospital and personal health record systems). In *2011 IEEE Conference on Open Systems* (pp. 406-410). IEEE.
5. Gao, X., Cui, Q., Shi, X., Su, J., Peng, Z., Chen, X., ... & Wang, N. (2011). Prevalence and trend of hepatitis C virus infection among blood donors in Chinese mainland: a systematic review and meta-analysis. *BMC infectious diseases*, *11*, 1-14.
6. Van Gorp, P., Comuzzi, M., Jahnen, A., Kaymak, U., & Middleton, B. (2014). An open platform for personal health record apps with platform-level privacy protection. *Computers in biology and medicine*, *51*, 14-23.
7. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2009). *Above the clouds: A berkeley view of cloud computing* (Vol. 17). Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.
8. Jabour, A., & Jones, J. F. (2013). Facilitators and barriers to patients' engagements with personal health records: systematic review. In *Universal Access in Human-Computer Interaction. Applications and Services for Quality of Life: 7th International Conference, UAHCI 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part III 7* (pp. 472-481). Springer Berlin Heidelberg.
9. Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. *IEEE transactions on computers*, *62*(2), 362-375.
10. Rachna, A., & Anshu, P. (2013). Maintaining Data Confidentiality and Security over Cloud: An Overview. *International Journal of Engineering Research and Applications (IJERA)*, *4*, 1922-1926.
11. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.
12. Wang, B., Li, B., & Li, H. (2014). Oruta: Privacy-preserving public auditing for shared data in the cloud. *IEEE transactions on cloud computing*, *2*(1), 43-56.
13. Jagadish, H. V., Ooi, B. C., Rinard, M. C., & Vu, Q. H. (2006). Baton: A balanced tree structure for peer-to-peer networks.
14. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet computing*, *16*(1), 69-73.
15. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2010). Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE transactions on parallel and distributed systems*, *22*(5), 847-859.