Data Security with Encryption and Private Key Using Multi Cloud Storage

Mr.Wasim S. Shaikh[1], Prof.Kishor N. Shedge[2]
Department of Computer Engineering
[1,2] Sir Visvesvaraya Institute of Technology, Nashik, India

Abstract- *Distributed computing has been imagined as the cutting edge engineering and answer for the rising stockpiling expenses of IT Enterprises. That implies Cloud loyally stores the information what's more, return back to the proprietor at whatever point it is asked. In any case, there is no assurance that information has kept up its uprightness. The research is center around cloud information stockpiling security, which has dependably been at the highest point of nature of administration. To guarantee the uprightness of information of clients in the cloud. As a major aspect of the confirmation procedure is expected that the TPA is dependable and autonomous as indicated by the administration level understandings (SLA), which does not imply that there is no space for the TPA to swindle. The methodology utilized for the encryption in the confirmation procedure was the blowfish algorithm. Extensive security and execution examination demonstrates that the proposed plan is very effective and strong against complex disappointment, malicious information adjustment assault, and significantly server intriguing assaults. The information in the cloud ought to be right, predictable, open and high caliber. Amid the previous few a long time, distributed computing has developed from being a promising business thought to one of the quickest developing parts of the IT business. So security identified with distributed computing is very important. The point of this examination is two crease one is guaranteeing the honesty of the information and second is giving the evidence that information is in anchored way.*

Keywords- Data storage, privacy-preserving, public auditability, cloud computing, delegation, batch verification, zero knowledge

I. INTRODUCTION

Cloud computing has been involved in every one's life "Cloud computing is a model for enable current ,convenient, on-demand network access to a shared pool of configurable computing resources which are rapidly released by minimum management effort or service provider interaction". In each platform there are more objects that affect the usage and the behavior, below some of these concerns in the cloud[1]. The cloud computing has been widely used in many organizations.

The small and medium scale companies use cloud computing services for many reasons, because storing data/file on cloud services provide fast access to their applications and reduce their hardware costs. Even most of us use cloud computing services on a everyday basis. For example, we use email systems (e.g. Yahoo and Google etc.) to exchange messages with others; social networking sites to share information and stay in contact with friends Even though because of these benefits the cloud lagging due to the integrity of data, data loss and by the attacks which falls it privacy[2]. Data integrity of the data is very important. Because data integrity guarantees that data is of high quality, precise, dependable and available.

II. LITERATURE SURVEY

The electronic currencies contains establishing ownership and ensuring anonymity with privacy which is generating and providing new currency. The Bitcoin can worth like our regular currency. The system create the track of the transactions also doubles as a minting mechanism. Lets consider some alternative mechanisms. Ripple [4] is also an electronic currency in which every user can issue currency.

However, The peers are form which accept only trusted issuer. In the network of electronics currency the chains are form between intermediaries and users for transactions. While in the KARMA currency a central authority is responsible for all transactions. Where as in the i-WAT currency there is no need of any central authority it consist of digital signature.

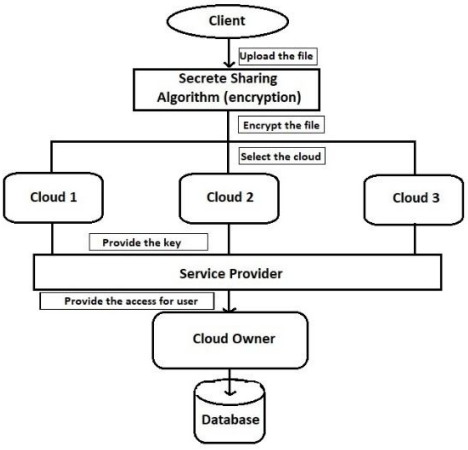
In this situation the function is using secret key for encryption which leads to difficult for the large amount of data. As for the small devices like PDAs mobile phones it become difficult to store large amount of data is they having limited computational power and also it become a storage overhead for a server and small hand held devices due to new inserted sentinels and error correcting codes[5]. The cloud service provider should provide a high end security and privacy on urgent basis.

Homomorphic encryption performs calculation on the ciphertext before decoding it first. Researchers anticipate this

promising procedure would be of huge help in actualizing numerous future distributed computing applications examine about registering productive also, exact outcomes for the SUM and AVG inquiries utilizing a protected, present day homomorphic conspire. Homomorphic encryption is computationally costly and because of its reliance on people in general key cryptosystem, it is hard to actualize.[8] From the perspective of data security, which has always which has always been an important aspect of quality of service.

III. PROPOSED SYSTEM

A proficient and secure dynamic inspecting convention, which can meet the above recorded necessities. To tackle the information security issue, our strategy is to produce a scrambled confirmation with the test stamp by utilizing the Bilinearity property of the bilinear blending, to such an extent that the inspector can't unscramble it yet can check the rightness of the verification.[9] Without utilizing the cover procedure, our strategy does not require any confided in coordinator amid the cluster reviewing for numerous mists.[4]



Fir 1.System Architecture

The server register the confirmation as a halfway estimation of the Verification, with the end goal that the reviewer can straightforwardly utilize this middle of the road incentive to check the accuracy of the evidence. Along these lines, our technique can incredibly lessen the registering heaps of the examiner by moving it to the cloud server.

A Modules of Proposed System

The system architecture of Secure Cloud Storage is shown in figure 1 and its modules are mentioned as below Modules of proposed system are as shown below

1) User

User of the data can be a business association or a single person who is storing its data on cloud. The system runs for handling the database of user and the formation of comma separated file which makes strong security.

2) Cloud Middleware

The middle ware is work under cloud service provider for storage and auditing of the data. A single system is needed to handle the middleware task which will reduce hardware requirement.[9] Which is discussed in next point.

3) Encryption

This system will accept normal data then it will encode the given data, after encoding it will provide encrypted data in cipher text [5], which is processed as this system deals with the database of ERP or organization's transactional data in real time, such as encrypted fields, records, rows, or column data in a database. The file is encrypted with the help of Blow fish Algorithm which is discussed in part B.

B Algorithm

The operations on files must be quick and fast. Hence by considering with other algorithms like DES and 3DES. The blowfish algorithms performance is high. The time taken to encrypt a file of 265 MB DES requires 10-11sec,3DES requires 12sec whereas Blowfish requires 3-4sec.Similarly DES operate on 22-23MB per sec,3DES operate on 12MB per sec whereas Blowfish operate on 64MB per sec which is a high performance. Hence the Blowfish is used in current work, as explained below

The blowfish algorithm is a symmetric block cipher it is having a key of variable length from 32 bits to 256 bits. It is freely available which perform operation on size 64 bits block and having 16 cycles for encryption. Significantly it is faster than other Encryption Algorithms.

The Blowfish Algorithm:

- Manipulates data in large blocks
- Has a 64-bit block size.
- It is having a key of variable size from 32 bits to at least 256 bits.
- Utilizations straightforward activities that are proficient on chip. e.g., restrictive or, expansion, table query,

measured duplication. It doesn't utilize variable-length moves or bit-wise stages, or restrictive hops.

- Employs precomputable sub keys. The sub keys are precomputed for the large memory system.
- Comprises of a variable number of emphasess. For applications with a little key size, the exchange off between the intricacy of a savage power assault and a differential assault make a substantial number of emphasess unnecessary. Consequently, it ought to be conceivable to decrease the quantity of emphasess with no loss of security (past that of the diminished key size).
- It uses the sub keys that are a one way to` hash of the key. This allow to create large key for data.
- Has no direct structures that lessen the unpredictability of comprehensive inquiry.
- Uses a plan that is easy to get it. This encourages examination and increment the trust in the calculation. By and by, this implies the calculation will be a Feistel iterated block cipher.

IV. RESULT AND DISCUSSIONS

The proposed system consists of ERP System. Through ERP we have to add files in the clouds. After uploading we will login to cloud and will check the data. And if suppose someone has hacked our account and made some changes or edit any data we will get alert to users mail that particular file has changed with its ID.

This framework will acknowledge typical information then it will encode the given information, subsequent to encoding it will give scrambled information in figure content, which is handled as this framework manages the database of ERP or associations value-based information continuously, for example, scrambled fields, records, lines, or segment information in a database.

Fig. 2. Encryption

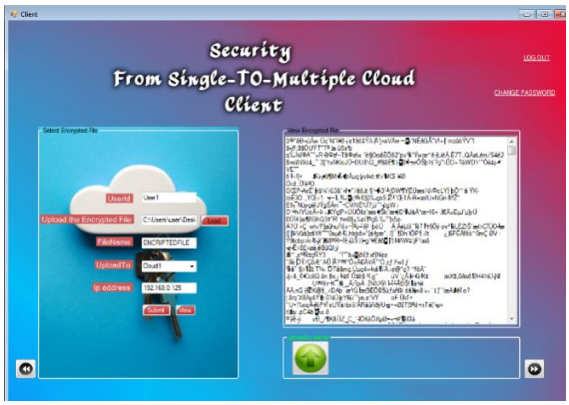


Fig. 3. Client Side

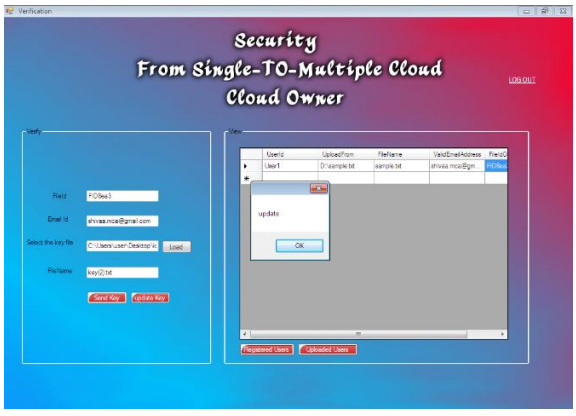


Fig. 4. Verification

V. AREAS OF APPLICAATION

A standard encryption calculation must be reasonable for a wide range of uses

1) Bulk encryption

The calculation ought to be productive in scrambling information records or a consistent information stream.

2) Random bit generation

The calculation ought to be effective in creating single irregular bits.

VI. CONCLUSION

The database of the system is secured with the help of encryption and by using SOAP protocol. The data is encrypted on one click and stores on cloud. For other people who viewing the data it is in the form of encrypted. The log file is generated to keep track of accounts. TPA is used for the Auditing of data and for alerting to the data owners for any malicious activity. The cloud computing technology is advantage for humans to achieve system resources and security services. The system help full for the business decision makers to analyse security challenges.

REFERENCES

[1] B.L Adokshaja and S.J Saritha, "Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm", ICECDS,2017.

[2] Yong Yu, Man Ho Au,"Identity Based Remote Data Integrity Cheking with perfect data privacy preserving for cloud storage", IEEE trans.4,april,2017.

[3] T.Subha and S.Jayashri, "Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security", IEEE ICoAC, 2016.

[4] Yuchuan Luo, Ming Xu and Shaojing Fu," Efficient Integrity Auditing for Shared Data in the Cloud With Secure User Revocation", IEEE 2015.

[5] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud sorage", IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp.1931-1940,Aug 2015.

[6] AFu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Trans. 2015.

[7] Johann Mitlohner, Sebastian Neumaier, "Characteristics of open data CSV file",UOEB 2015.

[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage", IEEE Trans Comput, vol. 62, no.2, pp.362-375,Feb,2013.

[9] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud", IEEE Internet Comput., vol. 16, no. 1,pp.69-73,jan 2012.