A Survey Paper on Data Confidentiality and Security in Cloud Computing using KIST Algorithm

Vasant N. Dhatrak[1] Jeevan R. Heda[2] Adesh V. Bhabad[3] Gaurav P. Shahane[4] Bajirao S. Shirole[5]
[1,2,3,4]B.E Student [5]Asstistant Professor
[1,2,3,4,5]Sanghavi College of Engineering, Nashik

Abstract— Now days rapidly increased use of cloud computing in the many organization and IT industries and provides latest software solution with minimum cost. So the cloud computing give us number of benefits with minimum cost and of data accessibility through Internet. The ensuring security risks of the cloud computing is the main factor in the cloud computing environment, The evolving essence is Cloud computing, that is beneficial in cost effective parts, such as capability inflexible computing, decreasing the time period to market and insufficient computing power. By using the complete ability of cloud computing, data are transmitted, processed and stored on the outside cloud service providers. The fact is that, the owner of the data is feeling extremely unconfident to locate their data outer to their own control. Security and Confidentiality of data stored in the cloud are key setbacks in the area of Cloud Computing. Security and Confidentiality are the key issues for cloud storage. This paper proposes a KIST encryption algorithm to concentrate on the security and Confidentiality issues in cloud storage and also compressed cipher text data in order to protect the data stored in the cloud.

Key words: Cloud storage, Security, Confidentiality, Cryptography, KIST Algorithm, Encryption, Decryption, Fraud Detection

I. INTRODUCTION

Cloud computing is the aggregate term for a gathering of IT advances which in cooperation are changing the scene of how IT administrations are given, gotten to what's more, paid for. A percentage of the supporting advances have as of now been accessible for a long while, however it is the mix of a few advances which empowers a entire better approach for utilizing IT. Cloud computing is a model for empowering advantageous, on-interest system access to a common pool of configurable computing resources (e.g., systems, servers, storage, applications, administration). In this paper proposes a KIST algorithm with an encryption technique for data security and confidentiality in the cloud storage. In the system user can store the data with the help of encryption technique on given cloud and provides alertness message to authorized user in case of data modification

A. *KIST Algorithm Characteristic:*

- An asynchronous key sequence is utilized which relies on a starting key and plain text
- A Splay tree is utilized so the substitution is progressive (dynamic).
- The encryption is quick and requires less space.
- Cipher text is compressed in most cases.
- The block size of the plain text and key size is flexible.
- It is useful for message integrity.

This algorithm makes use of an asynchronous key series and splay tree for encryption. This Encryption approach provides better key management approach for validating the users in the cloud. Cloud computing is likewise described as "On-demand computing" in light of the fact that the client can access according to their necessity and interest.

II. LITERATURE SURVEY

Key management and access control are significant for safe and secure cloud computing. This paper presents an encryption algorithm called Key Insertion and Splay Tree Encryption (KIST) approach shows good performance and provides significant results in terms of the security, time cost, space cost etc.[1]. The Encryption algorithm KIST which is based on the splay tree an asynchronous key sequence is used to change the tree dynamically and secretly. It is very efficient in the usage of both space and time complexity and also key encryption technique is done[2]. For securing the database of ERP on cloud with help of encryption and SOAP protocol. It has become easy to encrypt as well as upload the data simultaneously on cloud and also comparison of data is done if a change which gives alert which gives alert sending messages on Email –ID [11].

III. SCOPE AND OBJECTIVE

A. *Scope:*

Strong security to ERP clients for mass database is given utilizing Encryption process. It assists the client with reducing the work of storing the large database, i.e. browsing so as to select the database from the client's system and transferring database on CSP's server. The client sends all the information in a mass to the middleware on a single tick for storing automatically and encryption procedure is performed. After Encryption prepare the information will be store in Cloud Service Providers (CSP) database and Compare button will review the encoded information and contrasts that information and the first information, and if any modification are recognized then Compare button gives an alarm to clients through portable SMS and email alertness. The system will help to reduce the computational and storage overhead of the client and in addition to minimize the computational overhead of the cloud storage server.

B. *Objective:*

The objective of the system is to create secure cloud storage and information security at untrusted cloud service supplier and to overcome all issues like information verification and outsourcing the encrypted information and related troublesome issues. This system gives client a simple, proficient and dependable approach to secure information also as less equipment resources.

IV. PRESENT THEORIES AND PRACTICE USED

A. *Existing System:*

In existing outsourcing systems large volume of data created by numbers of users has been created significantly for uploading and retrieving the given data as per using KIST encryption algorithm. These KIST encryption algorithm provides better security and confidently for outsourcing the data. In given system encryption algorithm provide with highly reliable data. And that data gets encrypted plain text data to cipher text data and upload that data on given cloud (server) and also uploading that data needs while doing this in system with help of KIST algorithm an authorised person gets a key for accessing data it's for given authorised validation. Also these key gets validated then encryption techniques get performed, and backup cloud is also provided for data safety. That encrypted data again retrieved from given cloud into particular system into encrypted format due this it helps the user to keep data more secure and confident. Using KIST algorithm, key gets encrypted then with help of key gets generated and then that keys gets injected for performance. Due to this multiple user access the data randomly with full security.

B. *Proposed System:*

In proposed system solves security challenges for data in the cloud and provides a reliable and easy way to secure data with the help of encryption technology. In this system, the customer will get a proof of integrity of the data that he or she wishes to store in the cloud with bare minimum costs and efforts. Encryption process is performed with the help of KIST algorithm which will encrypt the plain data into cipher data and that ciphered data is uploaded on cloud. At the time of retrieval the ciphered data is again retrieved into plain data which is stored on system. This reduces the chances of getting discloser internally. In this manner, a relationship is established to cooperation model between operator and service provided to the users and also gives updating of given data, retrieved alert messages from cloud.

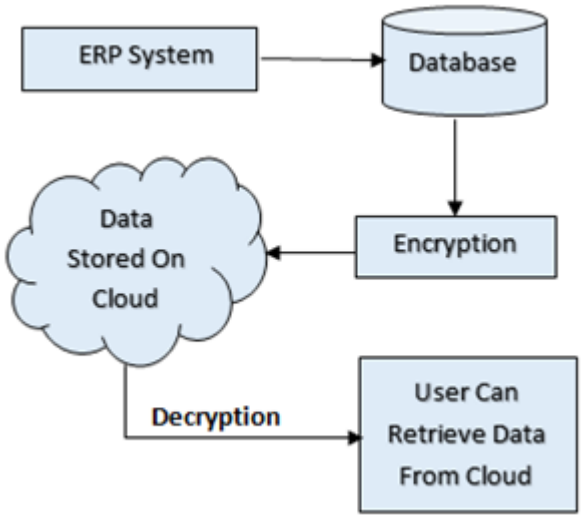

Fig. 1: Proposed System Architecture

C. *Proposed modules describes are as follows:*

1) ERP System / Other Data:

User may be an ERP system or business organizations who use cloud for data storage. An ERP system runs on a variety of computer hardware, software and network configurations, typically employing a database as a repository for information. The transformation of ERP into a cloud-based model has been shows the functionality faster is being moved to the cloud for data storage and computation management.

2) Encryption / Decryption:

This system will accept normal data, then it will encode or encrypt the given data, after encryption it will provide encrypted data in the form of cipher text from given cloud, 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 has per significant given. And other sensitive data like financial data, personal data, and other sensitive confidential data. Once encryption is done, then that cipher text will be deciphered by CSV (comma separate value) Parser. It will provide security for data.

3) Data Upload on cloud:

Using this part of architecture user data is uploaded (In this plain text data converted to cipher text data) on the cloud storage with help of encryption and decryption algorithm.

4) SOAP Protocol:

SOAP Protocol originally defined as "Simple Object Access Protocol" is a protocol specification for exchanging structured information in the implementation of web services in computer networks. This SOAP protocol is used for interfacing with Cloud Service Provider (CSP).The main idea behind SOAP was to:

- Improve Internet interoperability
- Integrate various business systems

V. CONCLUSION

The system is designed for securing the database of ERP and other sensitive data on cloud with the help of encryption algorithm and SAOP protocol APIs configuration. It has become easy to encrypt as well as upload data simultaneously on cloud on one click only that is scheduling. The data which are visible to the user on CSP is in Encrypted form. So here the hacker could not understand what exactly the information is or which record it is. On retrieving the data, the system will give original data and as well as CSV file is generated means a whole record of database is viewed as comma separated values. Log file describes the logged in details of, user or any other person who is trying to access the account. Compare button which gives the alert sending message (Email) from the Email Server on Email Id and also send text message on your mobile phone. It describes which data has been updated by hackers. But the best part is only data which is visible to hacker on the cloud is updated, the original data is not updated. So when user will get an alert user can again upload data on cloud and the original data is secure and protected from hacker.

ACKNOWLEDGMENT

We are thankful to IJSRD for giving us opportunity to present the paper in ther journal. We are also thankful to the Prof. Puspendu Biswas. (HOD of Comp. Engg. Dept.) for proper guidance and valuable suggestions. We are also greatly thankful Prof.Akshay Jain to other faculty members

for giving us an opportunity to learn and do this paper. If not for the above mentioned people, our paper would never have been completed in such a successfully manner.
We once again extend our sincere thanks to all of them.

REFERENCES

[1] A. Mercy Gnana Rani, Dr. A. Marimuthu , "Key Insertion and Splay Tree Encryption Algorithm for Secure Data Outsourcing in Cloud " ,in Proc. Of IEEE Computing and Communication Technologies (WCCCT), 2014 World Congress, ISBN: 978-1-4799-2876-7.
[2] R. Wei and Z. Zeng, "KIST: A new encryption algorithm based on splay", IACR Cryptology ePrint Archive, 2010.
[3] Abhinandan P Shirahatti, P S Khanagoudar, "Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing", in IMACST of NCACC-12 and NCETCT-2012, VOLUME 3 NUMBER 3 JUNE 2012, pages:161-171.
[4] Li, H.; Yang, Y.; Luan, T.; Liang, X.; Zhou, L.; Shen, X., "Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data" ,in Proc. Of IEEE Dependable and Secure Computing, IEEE Transactions on (Volume:PP , Issue: 99), ISSN : 1545-5971 , DOI: 10.1109/TDSC.2015.2406704 ,Date of Publication : 24 February 2015.
[5] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data".
[6] Mohit Marwaha, Rajeev Bedi "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing" in IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784, ISSN (Online): 1694-0814.
[7] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" in IJETCAS ISSN (print):2279-0047, ISSN (online) :2279-0055.
[8] Neha Tirthani, Ganesan R. "Data Security in Cloud Architecture Based on DiffieHellman and Elliptical Curve Cryptography."
[9] Dr. L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" in IJARCCE ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.
[10] Dr. Chander Kant, Yogesh Sharma "Enhanced Security Architecture for Cloud Data Security" in IJARCSSE Volume 3, Issue 5, May 2013 ISSN: 2277 128X.
[11] Shirole Bajirao Subhash, Dr Sanjay Thakur. "Data Confidentiality in Cloud Computing with Blowfish Algorithm" in IJETST- Volume 01, Issue 01, Pages01-06, March 2014. ISSN: 2348-9480.

