INTERNATIONAL ONLINE CONFERENCE ON ADVANCE RESEARCH & DEVELOPMENT IN ENGINEERING AND TECHNOLOGY

IO-CARDET 2016

E-ISSN NO:-2349-0721

Impact factor : 2.25

Secure Attribute Based Segmentation Technique for Cloud Structural Storage Data

Snehal Asare [1], Prof. Fazeel.I.Z.Qureshi[2]

[1]W.C.E.M, Nagpur [2] W.C.E.M, Nagpur

[1]snehal.asare241091@gmail.com [2] fazeel.zama20@gmail.com

ABSTRACT:

Cloud Computing is a new prototype for the IT industry Data security is one of the major question in cloud environment. The data owner do not control over the data after it gets uploaded on cloud. For data security we have to trust on security mechanism provided by other third party. We projects an outline in this the structural data i.e. datable get divided into different fragments according to their attributes. The data in each fragment can be encrypted by using different cryptographic algorithm and keys before storing them on the Cloud. The aim of this technique is to store data in a proper secure and safe way in order to avoid intrusions and data attacks meanwhile it will decrease the cost, time and storage space to store the encrypted data on the Cloud Storage.

Keywords— Cloud computing, Data security, Advanced Encryption Standard (AES), Segmentation, Data Encryption Standard (DES).

I. INTRODUCTION

Cloud computing is a computing environment where large group of remote servers are networked, which permits the central storage of data and it provides online access to computer resources or services. This computing environment permits enormous customer of cloud and service it allows its users to access this applications without installation it provides services ex- sending various files at any machine connected in a network with internet access. By centralized data storage processing and bandwidth provides more efficient computing. The various problems like sharing computing resources, users can easily solve their issues with the resources provided. By using cloud computing service, users can store their crucial data on servers and can access their data from anywhere they can with the Internet and do not need to worry about system collapse or disk faults, etc. Also, different users in one system can share their information and work, as well as play games together. Different Reputed companies such as Amazon, Google, IBM, Microsoft, and Yahoo provide the various cloud computing services. But being so useful, there are various problems faced by the cloud computing that can be classified as: Infected Application, Authentication, Data Verification, Availability, Data safety. To agreements with all these issue there was a need for a technique to handle all above issues and while supervise these issues, it should also enhance the security.

II. LITERATURE REVIEW

After lots of researches has made on cloud computing. We have referred various paper for our

research about various security models, data segmentation models, encryption algorithm. The piece of work focuses on how to acquire the security in cloud computing by slicing data done by Amit Khaparde. et al. in 2015 [1] .focuses on increasing the security of data in cloud environment by dividing data in the proper way and using various encryption techniques. His piece of work throw a beam of light on a new concept of partitioning, which segments the data and encrypt them as per there relevance. This idea not only enhance the security but be a hurdle in the way of attackers and hackers.

The author Vishwanath S. Mahalle et. al. [9] proposed a concept where the hybrid encryption is done to enhance the security of the data. The concept of using different algorithm form a hurdle for the attacker to access the vital data from the cloud. Even there will be no need to rely on the third party vendors for the security. This technique is used to make users data highly secured. We get benefit of both symmetric key and public key encryption which all together enhance security.

The author Devi, T et. Al. [10] presents the survey regarding data security in cloud computing and the analysis of each framework. These various frameworks gives the idea of various frameworks proposed uphill now there pros and cons. One of the framework deals with the data segmentation model .this models gives an idea to segment the data to increase the security.

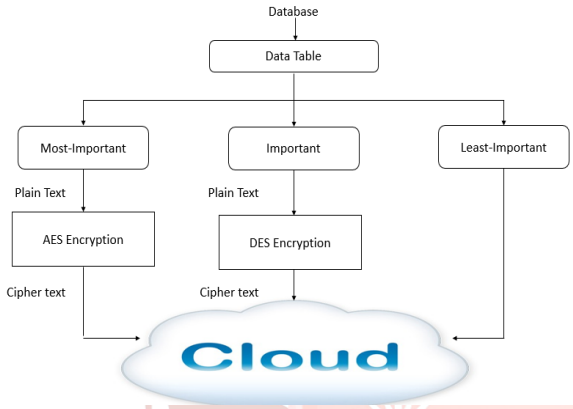
Aderemi A. Atayero [7], proposed an auditing system which is carried out in a way that the Third Party Auditor does its job without asking the copy of user's data. Also the Third Party Auditor is not capable of deriving the user's data while executing the auditing task. To verify the correctness of the cloud data on demand from the cloud users the Third Party Auditor is utilized, who without retrieving a copy of the whole data or introducing additional online burden to the cloud users performs the auditing. Block tag authentication is made to handle the data from the cloud storage efficiently. For the data that is present on the cloud database, there is need for remote data integrity check which guarantees the cloud users with a sense of security regarding their data. The third party audit ting has to be made obtainable in such a way that no additional burden is introduced to the cloud users. A single Third Party Auditor is capable of controlling multiple auditing tasks, which is achieved with the bilinear aggregate signature technique.

The author Prashant Rewagad et al. [14] propose an methodology for providing security in cloud network. These systems architecture uses the combination of digital signature algorithm (Diffie Hellman) and AES encryption algorithm. His piece of work utilized benefit of both authentication technique and key exchange algorithm blended with an encryption algorithm. This mechanism is known as "Three way mechanism" as it ensures all the three protection scheme of authentication, data security and verification, at the same instance.

III. SYSTEM STRUCTURE

In ABST approach, we need fragment the structural data which we need to store on the cloud. Structural data are those data which are well organized. All databases containing tables are one of the form of structural data. Thus, we are subdivide data table in various fragments. This separation is done according to the importance of the attributes. To extend security we use various encryption algorithm. Each fragments gets encrypted by the different encryption algorithm,

here we are using Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption. Encrypt each important fragment separately by encryption key, which motives to increase the protection of privacy and prevent its violation by the hacker, or even by the Cloud service providers themselves.



IV. PROPOSED TECHNIQUE

This dissertation proposed ABST (Attribute Based Segmentation Technique) to make structural data secure with less encryption time and storage space. In this technique a data table attributes gets encrypted according to their importance and stored on cloud. This attributes are the column exists in the table e.g. Employee table has attributes such as Name, Age, Phone number etc. which can be categorize as "Most-Important", "Important" & "Least/No-Importance". This attributes are categorized by their data owners. The data is then encrypted and stored on cloud. The aim of this suggested technique is to store data in a secure way which is accomplished by using Data Encryption Standard (DES) and Advanced Encryption Standard (AES) as per the data importance. "Most-Important" columns get encrypted by AES as it needs to be highly secured and "Important" columns (attributes) gets encrypted by DES and "Least-Important" columns kept unencrypted. Thus this mechanism will reduce the cost, storage space and time to store encrypted data on the Cloud storage center and also increases efficiency

V. CONCLUSION

Cloud computing has recently emerged as a paradigm for controlling and delivering services over the internet. Due to rise of its usage many challenges raised in this domain. Infected Application, Data protection, Availability, Authentication, Data Verification. All this stated problems are there because, there is no clear method to portioned data into various fragments and used different encryption algorithms according to the security of encryption algorithm. In this proposed ABST scheme we solve the problem of security and increase the security level of structural data than previous techniques. It also increase efficiency, reduce storage space and time.

REFERENCES

[1] Amit Khaparde."*An Approach For Securing Data On Cloud Using Data Slicing And Cryptography*"-2015

[2] Omer K. Jasim Mohammad "*Securing Cloud Computing Environment using a new Trend of Cryptography*"-2015

[3] Reza Fathi∗, Mohsen Amini Salehi†, and Ernst L. Leiss∗ "*User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services*"-2014

[4] Maghrabi, L.A. "*The threats of data security over the Cloud as perceived by experts and university students*"-2015

[5] Narula, S. , Jain, A. Prachi "*Cloud Computing Security: Amazon Web Service*"-2015

[6] Upadhyaya, A.; Bansal, M. "*Deployment of secure sharing: Authenticity and authorization using cryptography in cloud environment*"-2015

[7] Fei Chen; Tao Xiang; Yuanyuan Yang; Cong Wang; Shengyu Zhang "*Secure cloud storage hits distributed string equality checking: More efficient, conceptually simpler, and provably secure*"-2015

[8] Reiter, A.; Zefferer, T. "*Paving the Way for Security in Cloud-Based Mobile Augmentation*"-2015

[9]Vishwanath S. Mahalle "*Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm*"-2014

[10] Devi, T. , Ganesan R " *Data security frameworks in cloud*"-2014

[11] M. Sugumaran, BalaMurugan. B D. Kamalraj "*An Architecture for Data Security in Cloud Computing*"-2014

[12] Orner K. Jasim Mohammad, Safia Abbas, EI-Sayed M. EI-Horbaty : "*A Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment*" 2013

[13] Gruschka, N. ; Jensen, M. ; Iacono, L.L. ; Marnau, N. "*Security and Privacy-Enhancing Multicloud Architectures*" 2013

[14] Mr. Prashant Rewagad , Ms.Yogita Pawar. "*Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing*. In International Conference on Communication Systems and Network Technologies 2013.