NCRISET-2017 e-ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 2, No.6, 2017
www.ijies.net

Secured Data Over The Cloud Storage

Miss. Himanshi Agrawal[1], Miss. Nayan Chandekar[1], Miss. Sanchita Nirwan[1], Miss. Ashwini Khedekar[1], Prof.R.D.Kale[2]

[1]UG Student,[2] Assistant Professor,
Department of Computer Science Engineering,
G.H.Raisoni Institute of Engineering and Technology,Nagpur, India.

Abstract— *Cloud computing which is associate up growing technology needed a lot of security particularly once it embrace third party as service supplier. To overcome this issue AES (Advance Encryption Standard) that is encoding technique for cloud surroundings with trustworthy third party. Which can avoid the possibilities of whole information from obtaining hacked at a time and conjointly give access management and file secured deletion. Using the technique with AES (Advance coding Standard) can facilitate access solely authorized information to the approved user. This protocol is highly economical. By using this protocol is it can stop from any reasonably intrusion from any anonymous party, thus the overall outcome expected from this work are to supply security for the access of information in cloud surroundings.*

Keywords—Anonymous, AES(Advance Encryption Standard), Intruder,cloud storage, security.

1. INTRODUCTION

CLOUD storage is being widely adopted due to the popularity of cloud computing. However, recent reports [1],[2] indicate that data loss can occur in cloud storage providers (CSPs). Thus, the problem of checking the integrity of the info in cloud storage, which we have a tendency to referred to as secure cloud storage (SCS), has attracted a lot of attention. Secure cloud storage. This problem was first proposed by Juels and Kaliski [3] and Ateniese et al. [4]. Two main entities are involved in these protocols: a user and a cloud storage provider. A user outsources the data to the cloud who promises to store the data. The user then confirms the data integrity by interacting with the cloud using a secure cloud storage protocol.

Cloud computing is a model that permits Convenient Associate in Nursingd On-demand network access to a shared pool of configurable computing resources where uncountable users share an infrastructure.It offers many potential benefits to small and medium-sized enterprises (SMEs). It provides many services for

- Data processing
- Storage and backup
- Facilitate productivity
- Accounting services
- Communications
- Customer service and support

The database is keep in a table that has multiple records. These records may be categorized as follows:

- Explicit identifiers
- Sensitive identifiers.

Explicit identifiers are the attributes that identifies an individual. For e.g. Name, social security number etc.Sensitive identifier is the attribute with sensitive price. Here the value of the attribute isn't discovered to anyone. In banking, all the data is keep on the cloud. Cloud is an efficient and straightforward for sharing the info. With the help of AES (Advanced cryptography Standard) algorithmic program we are going to cipher the info.

2. OBJECTIVE

The main objectives are:
The attacker should not be able to hack the data. The main thing we can add about security i.e. anonymization encryption by AES (Advanced Encryption Standard) algorithm. We provide security so that no one can hack the data from database and cloud.

Propose a system which will not leave any path for entrant to intrude by exploitation “removal of identity technique”. Introducing anonymization to change the format of encrypted information inside few seconds anytime somebody tries to decipher it. We propose the semantic way to secure the data over cloud storage protocol based on any Banking data. As a result, we obtained a secured and verifiable secure cloud storage protocol. This project addresses the problem of confidentiality of dataset in cloud using Anonymization and accomplishes following:

- Minimize the risk of breaking privacy
- Limit the amount of information disclosure
- Develop greater public trust
- Perform dynamic mapping of dataset

3. LITERATURE REVIEW

Fei Chen, Tao Xiang, Yuanyuan Yang, and Sherman S. M. Chow [1] this paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time. Secure cloud storage was proposed only recently while secure network coding has been studied for more than ten years. Although the two areas are quite different in their nature and are studied independently, we show how to construct a secure cloud storage protocol given any secure network coding protocol. This

gives rise to a systematic way to construct secure cloud storage protocols.

Mazhar Ali, Saif U. R. Malik, Samee U. Khan [2] Off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud. Wholesale of data by cloud service provider is yet another problem that is faced in the cloud environment.

Arjun Kumar, Byung Gook Lee, HoonJae Lee [3] Cloud computing is the most demanded advanced technology throughout the world. It is one of the most significant topic whose application is being researched in today's time. One of the prominent services offered in cloud computing is the cloud storage. With the cloud storage, data is stored on multiple third party servers, rather than on the dedicated server used in traditional networked data storage. All data stored on multiple third party servers is not cared by the user and no one knows where exactly data saved. It is cared by the cloud storage provider that claims that they can protect the data but no one believes them. Data stored over cloud and flow through network in the plain text format is security threat.

Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, and Elisa Bertino[4],This paper proposes a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificate less public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks.

C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou[5]Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources.

4. PROPOSED METHODOLOGY

Module 1: Development of Login System/Page

We are developing Banking System Module in which bank staff will be able to login in his/her account. This module is similar to new user login page instead of password OTP and master key is mandatory.

Module 2: Development of OTP

In OTP creation module, we are generating random password through AES. Every time when user log's in into his/her account, a new OTP will be generated by this module and will be inform to user through the message on his/her registered mobile number.

Module 3: Data Sharing

To change information sharing within the Cloud, it is imperative that solely approved user's square measure ready to get access to information hold on within the Cloud. The administrator ought to specify a bunch of users that square measure allowed to look at his/her data. Any employee of the organization ought to gain access to the information anytime while not the information owner's intervention.

- No different user, apart from the information owner and also the members of the group, ought to gain access to the information, together with the Cloud Service supplier.
- The information owner ought to be ready to revoke access to knowledge for any member of the group.
- The information owner ought to be ready to add members to the group.
- No member of the group ought to be allowed to revoke rights of different members of the cluster or be a part of new users to the group.

The secure data sharing in clouds methodology provides:

1. Data confidentiality and integrity
2. Access control
3. Data sharing (forwarding) without using compute-intensive encryption
4. Insider threat security
5. Forward and backward access control.

The secure data sharing in clouds methodology encrypts a file with a single encryption key (master key). Two different key (OTP and Master Key) shares for each of the users are generated. The possession of a single share of a key allows the secure data sharing in clouds methodology to counter the insider threats. The other key share is stored by an authorized person.

Module 4: Data Anonymization

Introducing anonymization to change the format of encrypted data within few seconds each time someone tries to decrypt it.

Research Methodology:

The Main Security implementation of the concept is One Time Password our proposed system which generates a new OTP every time whenever an authorized user log's in into his/her personal account. Every time a new OTP is generated randomly. As soon as user inputs his/her username and password the 6 Digit OTP is provided to user through message on his/her registered mobile number. The Concept has been implemented in such a way that it adds high level of security to our proposed work.

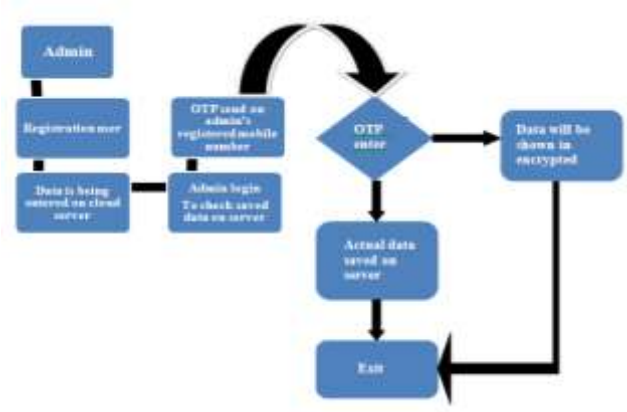


Fig 4.1:-Flow chart of propose system

AES (Advanced Encryption Standard) Algorithm:- AES is used for encryption and decryption of data. In cryptography, the Advanced Encryption Standard (AES) is also known as Rijndael algorithm.

- It is a block cipher with block length of 128 bits. It allows three different key length i.e. 128,192 or 256 bits. Each round of processing include one single bit based substitution, a row wise permutation, a column wise mixing steps and addition of round key.
- The project is to provide authentication and encryption by AES (Advance Encryption Standard) and provide a secrete key to access the encrypted data using the same.
- By using AES (Advance Encryption Standard) encryption and decryption we can either encrypt the desired data or the whole data.
- Data anonymization technique can provide confidentiality of data by letting only the authorized user se the data allotted to him.

AES consists of following steps:
Key Generation, Initial Round
Four different stages area used, one of permutation and three of substitution:

1st stage: **Substitute Bytes**

Uses S-box to perform a byte by byte substitution of the block.

2nd stage: Shift Rows

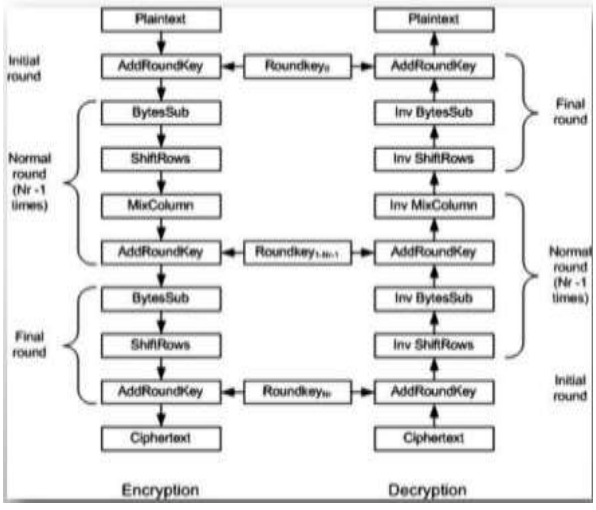
A simple permutation is performing row by row.

3rd stage: Mixed column

A substitution that alter each byte in column as a function of all of the bytes in the column.

4th stage: Add round key

A simple bitwise X-OR of the current block with portion of the expanded key



The Implementation of concept:

When the admin login from his system,he get a screen that simply prompts him to enter his username and countersign, Once he enter the username and countersign, the user is redirected to another screen where in conjunction with his countersign is prompted to enter the once countersign. Two different keys(OTP & Master Key) shares for each of the users are generated. The OTP has been delivered on to the users registered mobile number that admin had provided. The OTP is valid only time. Each time user login, a new OTP is generated and it has been send on registered mobile number of that user or employee. If the Master Key entered is wrong then the data is displayed in encrypted format. Thus this OTP becomes the most secure thanks to implement security in cloud and information as notwithstanding the countersign of the admin is compromised however victimization this OTP he's secure within the sense that the opposite countersign that he/she have to be compelled to log in can solely be sent on to his mobile.

EXPERIMENTAL RESULT AND FUTURE WORK

In this project we have provided the security to the data which is stored over cloud with the help of AES (Advanced Encryption Standard) and Anonymization technique in cloud to secure the data.

Till now for experimental analysis, private cloud has been used. In future Public cloud or hybrid cloud may be used with some more effective anonymization algorithms. The study of anonymization depends on many factors. Other anonymization algorithms may be implemented like binning, partitioning, swapping and random noise addition. The techniques that area unit presently safe for anonymization might fail in future. Still information anonymization could be a viable resolution that's extremely suggested for security in cloud. So, the offered techniques of anonymization could also be integrated to realize better results. An efficient tool for associate in anonymization will be developed that uses an integration of all offered anonymization techniques.

CONCLUSION

Cloud computing faces privacy and security issues. Cloud computing needs customary methodologies and technical solutions to access privacy risk and establish adequate protection levels. A robust protection ought to be ensured by organizations, agencies for personal information no matter the atmosphere wherever the information is truly keep. As a result of loss of this sensitive information might produce a negative impact for organizations. Anonymization may be a viable technique to secure cloud computing. It limits the misuse of sensitive information.

REFERENCES

[1] *Fei Chen, Tao Xiang, Yuan Yang, Sherman S. M. Chow "Secure Cloud Storage Meets with Secure Network Coding" IEEE INFOCOM 2014- IEEE Conference on Computer Communications, 978-1-4799-3360-0/14/.*

[2] *Mazhar Ali, Saif U. R. Malik,Samee U. Khan," DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transaction on journal name, manuscript ID IN 2015.*

[3] *Arjun Kumar, Byung Gook Lee, HoonJae Lee", Secure Storage and Access of Data in Cloud Computing" 978-1-4673-4828- 7/12/$31.00 ©2012 IEEE.*

[4] *Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, and Elisa Bertino," An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transaction on knowledge and data engineering VOL. 26, NO. 9, SEPTEMBER 2014.*

[5] *A. Juels and B. Kaliski Jr, "PORs: Proofs of retrievability for large files", Proc. ACM Conf. Comput. Commun. Security, pp. 584-597, 2007.*

[6] *Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou," Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transaction on parellel and distributed system, VOL. 25, NO. 1, JANUARY 2014.*

[7] *Luca Ferretti, Michele Colajanni, and Mirco Marchetti," Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases " IEEE Translation on parallen and distributed system, VOL. 25, NO. 2, FEBRUARY 2014*.

[8] *Khoi-Nguyen Le-Huu, Diem Ho, Anh-Vu Dinh-Duc," Towards a RISC Instruction Set Architecture for the32-bit VLIW DSP Processor Core" ", IEEE Transaction on knowledge and data engineering VOL. 24, NO. 2, NOVEMBER 2014.*