Different Levels of Security in Cloud

Prof. Pranali Kosamkar[1] Prachi Kadam[2] Shahista Shaikh[3] Rashmi Linganwar[4] Komal Mathpati[5]
[1]Assistant Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]MIT, Pune

Abstract— Cloud computing is mainly used for the security of data. Cloud stores a large number of data securely and very efficiently without the fail of service to the customer. Cloud is used by different organizations in a variety of different service models. But a number of security issues are associated with cloud computing. There are different security issues faced by cloud provider and different customers. This paper gives idea about the different levels of security provided by encryption technology. It gives overview about the cryptographic techniques which can be used to design the secure cloud service provider. Here we have discussed the layers of encryption used in various systems and the algorithms used for their implementation.

Key words: cryptography, levels of encryption, security

I. INTRODUCTION

Cloud computing is one of the strong and dominant technology in present situation. It offers services in least price manner than ancient approach. User will uses all services of cloud and share their information. It provides different characteristics such as device and location independence, scalability and elasticity, reliability, etc. Due to these characteristics the industries are shifting towards cloud. Cloud computing is used to store a huge amount of data and perform different computations. The cloud computing provides shared resources, data and information which is provided to computers and other devices on-demand so it is also known as "On-Demand-Service".. There are 3 types of service models such as infrastructure as a service, platform as a service and software as a service also known as IaaS, Paas and SaaS.

Now-a-days data security is a big issue. Cloud is a database that lets the users to keep the data confidentiality on public cloud. As data is stored on cloud and whole control over data is not in user hand, it is handled by cloud service provider. Cryptography is one of the technique used to keep the data secure. In cryptography there are mainly two techniques which are used to convert the original data into un-readable format (cipher-text), those techniques are:

A. Symmetric Key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. It is also known as secret-key cryptography. The main challenge in symmetric key cryptography is to exchange the key in secure way between sender and receiver. There are 2 types of Symmetric key Cryptography:

1) Stream Cipher

It encrypts the bytes of the message one at a time.

2) Block Cipher

It encrypts the no of bits as a single unit known as block.

B. Asymmetric Key Cryptography

Asymmetric key cryptography in which two different keys are used a public key and a private key. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. It is also known as public-key cryptography. It is more secure approach than secret-key cryptography because private key is not shared, so no need to exchange the key.

There are 3 types of services provided by the cloud:

1) Saas

In this methodology, the user doesn't purchase software package, however rather rents it for use on a subscription. So it is also called as pay-per-use model. User has to pay for the service. Example: Gmail , Google Drive.

2) Paas

In this method, the development environment is offered by the service provider to application developers or application vendors, who develop different applications and offers the services through the providers platform. Example: Google Gears, Microsoft Azure.

3) Iaas

In this method, the service provider offers server, storage and networking facilities to the user. The user should able to run any type of software of his own including operating systems. The service provider handles the physical infrastructure at a remote place and virtual abstractions are given to the users for their use. Example: Amazon Web Services, Google Compute Engine.

Different encryption levels are used to provide the security to the data. As the level of encryption increases the security of data also increases.

II. LITERATURE SURVEY

A. Single Layer Encryption

Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer has implemented "Database Encryption", in which they represents encryption and key management. In this paper, a pair of keys are generated for each user. These key pairs are separated when they are generated. The private key is placed at the client end by the user, while the public key is present in the database server. The database encryption is done by using the RSA public-key scheme and also it provides two database encryption schemes: one column oriented and the other row oriented. It should be possible to encrypt only sensitive data while keeping insensitive data unencrypted[1]. The Cipher Cloud is a framework that allows the users to keep their data confidentially on the public cloud. To achieve confidentiality, Cipher Cloud uses a two step encryption process : first, all the data sent from client to cloud or vice versa is kept totally in the encrypted form. For this encryption different encryption algorithms are used like - AES, DES, RSA and Blowfish to achieve the security of data on the cloud. DES is developed in early 1970s; Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001.All of these algorithms

are symmetric algorithms, in which only a single key is used for encryption or decryption purpose. But RSA is asymmetric key algorithm, created by Ron Rivest, Adi Shamir and Lenard Adleman in 1978 which used for public key cryptography. In this, two public and private keys are used for encryption/decryption There is no confusion of keys at user side. The data is decrypted at server side only.The requested users are not authenticated so an unauthorized person can make the misuse of data[2]. Baojiang Cui, Zheli Liu and Lingyu Wang has implemented "Single level security" in which they stored encrypted data on cloud. They used Key-aggregate searchable encryption (KASE) to support searchable group data sharing functionality, which means the user may select some group of files and share it with a group of selected users, then it will allow to perform keyword search on that files. First, a data owner distributes a single aggregate key (rather than a group of keys) to a user for sharing the group of files. Second, the user has to submit a single aggregate trapdoor (rather than a group of trapdoors) to the cloud for performing keyword search over any number of shared files. In this scheme we can use any encryption algorithm i.e. AES,DES, RSA, etc[3].

To provide the security to the uploaded data, Deepika Verma and Er. Karan Mahajan have used two security algorithms Diffie-Hellman Key Exchange and TDES algorithms in combination with RBAC method. These two algorithms are used to encrypt the data. Diffie-Hellman algorithm is used for the generation of keys for secure key exchange[4].

Dr. L. Arockiam, S. Monikandan had worked on "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", and have proposed the model which provides "Single layer security". They have proposed a symmetric algorithm which consists of two steps: encryption and decryption. They have stated that the data is first encrypted with the help of a symmetric key and the same key is used at the time of decryption when the user demands the access to the data. This symmetric key is provided only to the authentic user for the decryption of data [5].

B. Two Layer Encryption

To provide more security two layer encryption technique is used. In 1st level data is encrypted using AES algorithm which is mainly used to authenticate the data.2nd level establishes a secure connection between end-users and cloud servers for user authentication, data transmission, access controls using RSA algorithm. They also provided with an independent middleware (Agent) to perform the process of user authentication, access control, and data protection in cloud servers[6]. In "Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication", the authors of this paper have proposed two layers of security. They have used two clouds while implementing the system i.e. public cloud and private cloud. In this two way authentication system, private cloud will be consisting of the sensitive information about the users and the keys associated with the data and the public cloud will contain the actual data to be stored in cipher text form. In this system, they have used AES algorithm to encrypt the data. While delivering to the end users, this method enhances the security of the data with the help of hybrid algorithm. Firstly the data uploaded on the cloud server is converted into cipher text. This data is decrypted with the secret key provided to the user in mailbox. This system has the potential to be useful in commercial situations and provides secure data storage in the cloud enforcing the access policies[7].

Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi have implemented a data security method using Elliptic Curve Cryptography. They have used two security solutions i.e. authentication and encryption for secure data transmission from one cloud to another cloud. This Elliptic Curve Cryptography technique includes two operations that are key generation and encryption. First of all, the keys are generated. It calculates hash function for the data. Data is encrypted using keys. On the receiver side, the signature is verified and the data is decrypted[8].

C. Multilayer Encryption

Multilayer encryption provides the security at different levels such as service provider level, third party level, user level, and network level, etc. Kanupriya, Meenakshi Sharma have described the security levels in 4 steps. First is Categorization in which data is classified. Second is Data Encryption and Decryption for this standard algorithm like RSA, AES are used for encryption and decryption. Third is Data Integrity to check whether data is tampered or not for this they are using MD5 algorithm. Fourth is Role Based Dual User Authentication is used for user authentication and verification is carried out by third party and further it is verified by data owner[9]. The levels for database encryption granularity are database-level, table-level, record-level and field- level. It gives the method for encryption of these levels. In database level, they have given two method that are kernel layer and outer layer encryption and the second one is design of data encryption engine and encryption dictionary. In this encryption granularity level whole database is encrypted. In table level, the tables in the database are used as basic unit of encryption. The table-record level is for encrypting the data which is present in the form of records in the tables of database. The field level encryption is used for the encryption of sensitive fields in the database tables[10].

In "Multilevel Threshold Secret Sharing in Distributed Cloud", the user's data is splited into multiple parts and each part is stored on different clouds at different locations using threshold secret sharing methods. There are two multilevel threshold secret sharing schemes .In the first level of the secret sharing scheme, the secret key is splited into parts and distributed it at multiple cloud service providers. The second level consists of splitting each sub-key into multiple numbers of sub-secrets keys at each cloud service provider. They have generated a share pool which is used to determine the number of keys at each cloud service provider using Chinese Remainder Theorem (CRT).We have to create multiple keys for one file because it is distributed[11].Jun Zhou, Zhenfu Cao, Xiaolei Dong and Xiaodong Lin has implemented "Multilevel security" for the e-healthcare system. They have proposed this system so that the patient's private and sensitive information can be stored securely on e-healthcare cloud. In this paper, they have proposed construction of "a white-box traceable and revocable multi-authority attribute-based encryption named

TR-MABE" for fine-grained multiple level access control in e-healthcare cloud computing systems. They have used algorithms such as GlobalInit, CASetup, AASetup, Encrypt, CAKeyGen, AAKeyGen, Decrypt and Trace[12].

HoWon Kim and Sunggu Lee have implemented a crypto processor composed of a 32-bit RISC processor and coprocessor blocks. They have used the algorithms AES, RSA, SEED, triple-DES, and ECC. The coprocessor blocks of the crypto processor are designed to accelerate private and public key crypto algorithms. Fast execution of various security applications is possible because of the programmability of the crypto controller[13]. To avoid the violation due to collision attack and heavy computation, in "Multi owner based data security in cloud using threshold cryptography", the authors have proposed system which uses threshold cryptography. In this technique data owner Divides users in groups and provides a key to each user group for decryption of data. part of the key is shared with each user in the group. in this proposed system There are multiple owners of keys. They have also proposed a term Onetime session password (OTP) which is shared between user group and data owner. It is used for the authentication of users. They have mentioned that the key is encrypted using Deffie-Hellman algorithm which is used for the security in transfer of file[14]. In "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", authors have proposed the method containing three parts: Private Key Generator (PKG), Trusted Cloud (TC), and User. The Private key generator is used for generating users' keys. The infrastructure is rent by user from trusted Cloud to save his data. This system is proposed to provide more secure method for data protection. It also reduces the complexity of management with the help of IBC. ECC is used for providing data confidentiality and Elliptic curve digital signature algorithm (ECDS) for data integrity. The main idea of this system is to use the combination of the security of IBC and ECC with Trusted Cloud (TC). TC also decreases the denial of service attack (DOS) on CSPs [15].

III. Conclusion

In this paper, we have discussed about the need of authentication in cloud computing. Security and Privacy of data in Cloud Computing is an area which has a full of challenges and importance. Different cryptographic techniques are used to provide secure communication between the user and the cloud server. To handle the encryption of large amount of data in cloud storage symmetric encryption is used to increase the speed and computational efficiency. This paper has discussed different levels of security for providing more secure data on the cloud. Levels of security is provided with the help of different encryption and decryption techniques. The algorithms are used to encrypt the data of user in cloud. By applying this encryption algorithm and increasing the levels of security, user ensures that the data is stored only on secured storage i.e. cloud and it cannot be accessed by un-authenticated administrators or intruders

References

[1] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer, "Database Encryption – An Overview of Contemporary Challenges and Design Considerations", SIGMOD Record, September 2009 (Vol. 38, No. 3).
[2] Manpreet Kaur, Rajbir Singh "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013.
[3] Baojiang Cui, Zheli Liu and Lingyu Wang "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on Computers, vol. 6, No. 1, January 2014.
[4] Deepika Verma, Er. Karan Mahajan "To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms", International Journal of Advances in Science and Technology (IJAST) Vol 2, Issue 4 (December 2014).
[5] Dr. L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[6] Mohammad Ahmadi, Mostafa Vali "A Reliable User Authentication and Data Protection Model in Cloud Computing Environments",International Conference on Information, System and Convergence Applications June 24-27, 2015 in Kuala Lumpur, Malaysia.
[7] Harpreet Singh, Er. Gagandeep Singh, Er Madhu Bahl "Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-7).
[8] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering(IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 .
[9] Kanupriya, Meenakshi Sharma "Level-Based Data Security Model in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-4 Issue-2, July 2014.
[10] Zhou Yuping and Wu Xinghui, Information Science and Technology School Hainan Normal University Haikou , Hainan, China, "Research and Realization of Multi-level Encryption Method for Database".
[11] Doyel Pal, Praveenkumar Khethvath, Johnson P. Thomas, Tingting Chen, "Multilevel Threshold Secret Sharing in Distributed Cloud"
[12] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin TR-MABE: White- Box Traceable and Revocable Multi-authority Attribute-based Encryption and Its Applications to Multi-level Privacy-preserving e-Healthcare Cloud Computing Systems, 2015 IEEE Conference on Computer Communications (INFOCOM).
[13] HoWon Kim, Member, IEEE, and Sunggu Lee, Member, IEEE, "Design and Implementation of a Private and Public Key Crypto Processor and Its

Application to a Security System", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY 2004.

[14] Sagar Rakshe, Rushikesh Suryawanshi, Sachin Tandale, Onkar Thorawade, "Multi owner based data security in cloud using threshold cryptography: A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 10, October 2015.

[15] Asst. Prof. Dr. Salim Ali Abbas,Amal Abdul Baqi Maryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.

