A Review of Sharing and Storing Of Data over Cloud Computing Using Cryptography Technique

Madhuri Mishra
M.Tech Scholar, Department of CSE
CSE, Jhansi INDIA
E-mail- madhurimishra.16@gmail.com

Somya Jaiswal
Associate Professor, Department of CSE
CSE, Jhansi INDIA
E-mail:- somyacs0089@gmail.com

ABSTRACT
Cloud computing play an important role in development of IT based services and application. The utility and diversity increasing day to day in various sectors such as health care, agriculture and many more discipline. The sharing and storing of data over cloud network always faced threats of security. For the improvement of security strength of user side and cloud network used various cryptography technique. The cryptography technique provides various key cryptography technique some are based on symmetric and some are based on asymmetric key cryptography technique. In this paper presents the review of cloud data sharing and security issue. In concern of security issue now a day's used public data auditing concept over cloud network.

Keywords: - Cloud computing, data sharing, cryptography, Message Digest (MD).

INTRODUCTION

The data integrity and security is important issue in cloud computing environment. The integrity of data basically depends on the cloud service provider and user [1]. Now a day's most of user faced a problem of security threats by tried party and another medium. For the improvement of security over cloud computing used various security model and access control technique. The access control technique basically depends on the level of user access [2, 3]. The primary user of cloud computing has certain limited number of permission of accessing of data. The data storage over cloud computing is always a challenging issue in concern of retrieval and editing of data [5]. One of the big challenges is verifying the integrity of the data because users cannot know how the cloud storage service handles their data. These cloud storage services are provided by commercial enterprises, so it cannot be fully trusted by users. Therefore, the cloud service provider may hide data loss and data errors in the service because their benefits. It is very serious when a user stores data in untrusted cloud storage, for example, a large size of the outsourced data and the client's limited resource capability, and the client how to find an efficient way to achieve integrity verification without the local copy of data files [6]. The term cloud encompasses a variety of distributed computing environments, varying with respect to the architectural or trust assumptions and the services offered. In particular, the US National Institute of Standards and Technology distinguishes four deployment models and three service models. The deployment models range from a private cloud, where the infrastructure and services are operated for a single organization and are maintained on a private network, to a public cloud, where the infrastructure is made available to the public and is owned by an organization offering cloud services. For the sharing of files over cloud computing used key cryptography technique. the key cryptography technique used the concept of sharing of key in public and private mode. Section II discusses about cloud computing and data security, Section III discusses about the related work. Section IV discusses problem formulation and finally, concluded in section V

II CLOUD COMPUTING AND DATA SECURITY

Mostly the security issues which arise in Cloud Computing are the result of users/enterprises lack of control on the physical infrastructure. Enterprises mostly don't know where their data is physically stored and which security mechanisms are in place to protect data i.e. whether the data is encrypted or not and if yes, which encryption method is applied also if the connection used for data to travel in the cloud is encrypted and how the encryption keys are managed [9].

- Technical security issues in Cloud Computing, however, these issues are more related with the problems of web services and web browser and not of Cloud Computing. These issues are still very important to Cloud Computing as Cloud Computing makes a lot of use of web services and users rely on web browsers to access the services offered by the cloud. The common attacks on web services include the XML Signature Element Wrapping, where XML signature is used for authentication.
- Browser Security is also an important issue in Cloud Computing as in a cloud most of the computation is done on remote servers and the client PC is only used for I/O, and authorization of commands to cloud. Hence, standard web browser was a need of situation to send I/O and this was utilized by different names: web applications, web 2.0 or Software as Services (SaaS). However, the use of

web browser raised the question of security [5]. TLS (Transport Layer Security) is important in this matter as it is used for host authentication and data encryption. XML signature or XML encryption cannot be used by browser directly as data can be only encrypted through TLS and signatures are only used with the TLS handshake. Hence, browser only serves as a passive data store.

III RELATED WORK

In this section discuss related work in the field of data sharing over cloud computing environment. The sharing of data over cloud computing faced a problem of data integrity and data isolation. For the integrity of data used various algorithm by different authors discuss here.

Neetu Kishore and Seema Sharma [1] Et al. The migration of sensitive data to a public cloud domain has risks associated with data loss, information theft, confidentiality and other vulnerabilities. There are security measures deployed at multiple points but the question of secured end to end data transmission still remains unanswered. While there are different security measures for data protection in the common computing environment, the Cloud architecture needs new techniques for security. It is important to realize that from a scientific standpoint, there is no absolute notion of security.

Kajal Chachapara and Sunny Bhadlawala [2] Et al. Cloud user can generate keys for different users with different permissions to access their files. This framework uses cryptography algorithms like AES and RSA. AES is most secure algorithm in cryptography. Once key is generated user can provide that key to decided user. So when decided user will try to access files on cloud with that key, permission decided by owner will be given to that user. This is partial access to user and more secure then providing password to user. Cloud service providers can also add concept of defining files also like cloud user can generate key for particular file, particular user and particular permission. As per the key generation steps, first we will have to take a secret code from user, then we will generate 128 bit key using an AES algorithm. Then we will have to take a name of user for whom key is being generated and permission that we want to provide. Final outcome will be encrypted again with RSA algorithm.

Preeti Garg and Dr. Vineet Sharma [3] Et al. Due to increasing use of mobile devices the requirement of cloud computing in mobile devices arise, which gave birth to Mobile Cloud Computing. Mobile devices do not need to have large storage capacity and powerful CPU speed. Due to storing data on cloud there is an issue of data security. Because of the risk associated with data storage many IT professionals are not showing their interest towards Mobile Cloud Computing. In this scheme encryption is used to provide security to the data while in transmit. Because the encrypted file is stored on the cloud, so user can believe that his data is secure. In the scheme file, only in encrypted form is transferred over the channel, which reduces the problem of information disclosure. No, third person or intruder can get the file because that person do not knows the key of data owner.

Syam Kumar Pasupuleti, Subramanian Ramalingam and Rajkumar Buyya [4] Et al. In this paper, we propose an efficient and secure privacy-preserving approach for outsourced data of resource-constrained mobile devices in the cloud computing. Our approach employs probabilistic public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. We aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the file retrieval accuracy.

Victor Chang, Yen-Hung Kuo and Muthu Ramachandran [5] Et al. In penetration testing, CCAF multi-layered security could detect and block 99.95% viruses and Trojans and could maintain 85% and above of blocking for 100 hours of continuous attacks. Detection and blocking took less than 0.012 second per Trojan and viruses. A full CCAF multi-layered security protection could block all SQL injection providing real protection to data. CCAF multi-layered security had 100% rate of not reporting false alarm. All F-measures for CCAF test results were 99.75% and above. How CCAF multi-layered security can blend with policy, real services and blend with business activities have been illustrated. Research contributions have been justified and CCAF multi-layered security can offer added value for volume, velocity and veracity for Big Data services operated in the Cloud.

Alessio Botta, Walter de Donato, Valerio Persico and Antonio Pescape [6] Et al. The integration of Cloud Computing and Internet of Things (IoT) represents the next big leap ahead in the Future Internet. The new applications arising from this integration – we called CloudIoT– open up new exciting directions for business and research. Since the adoption of the CloudIoT paradigm enabled several new applications, we derived the main research challenges of interest for each of them. We further analyzed such challenges in order to identify current research directions. Finally, we surveyed available platforms and projects by comparing their main aspects and identified open issues and future research directions in this field.

P.Vijaya Bharati and Dr. T.Sita Mahalakshmi [7] Et al. Initially every 16-bit sequence is changed according to a random permutation matrix using a random sequence generator. And then HMAC-SHA512 is used to generate a hashed message authentication code to secure the data-in-transit. Later on encoding of the data is implemented using Information Secured Algorithm (ISA) in which the information is treated as sequences of elements. The message is divided into blocks and each block is labeled. For encoding, we consider l-sequences which are the cipher blocks. The blocks are such that the message can be recovered from any m of the n blocks. The encoding is done using an n by m matrix. Decoding also involves few

mathematical operations reconstructing the matrix from column vectors. The data stored as encoded data with ISA and HMAC-SHA512 generated code.

Vishal R. Pancholi and Dr. Bhadresh P. Patel [8] Et al. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as AES (Advanced Encryption Standard). It is based on several substitutions, permutation and transformation. AES encryption is the fastest method that has the flexibility and scalability and it is easily implemented. On the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption method.

Wei-Fu Hsien, Chou-Chen Yang and Min-Shiang Hwang [9] Et al. Because users' data is stored in the cloud storage service, it brings users' data security issues. In the public auditability model, users can delegate the third party auditor to verify their data is efficient. According to the literature, we sort out the basic requirements in public auditability, which can be classified to the case for your application.

Kamlesh Kumar Rao and Sanjay Kumar Yadav [10] Et al. Data and computation integrity as well as security are major considerations for end users of Cloud computing facilities. Today's clouds typically place centralized, universal trust in all the cloud's nodes. This simplistic, full-trust model has the negative consequence of amplifying potential damage from node compromises, leaving such clouds vulnerable to myriad attacks. Unfortunately, adopting cloud computing has required users to cede control of their data to cloud providers, and a malicious provider could compromise with data's confidentiality and integrity. Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client.

Pierangela Samarati and Sabrina De Capitani di Vimercati [11] Et al. With the rapid growth of cloud computing platforms and services, cloud security is becoming a key priority for all players. In this chapter, we presented an overview of security issues and concerns in cloud scenarios, illustrating their impact on the confidentiality, integrity, and availability properties and describing current solutions and possible challenges and directions.

S. R. Vijayalakshmi & S. Muruganand [12] Et al. system includes two aspects hardware and software. The hardware is composed of one base station with RS232 & XBeepro and several sensor nodes. The sensor node and base station control module are designed. The software aspect is mainly consisting of one monitoring center/ base station that can supervise all the location, through the information given by all the nodes inside the whole network. The front end solution is the easy way to integrate the IoT and WSN for environment monitoring.

IV PROBLEM FORMULATION

In this section discuss the security issue of cloud computing. The cloud computing environment used the process of data sharing over the network. The sharing of data over the network faced a problem of security threats. The security threats raised in both side user access side as well as service provider side. The security process maintains three parameter availability, integrity and confidentiality [10].

1. Protection of data at rest
2. Fine-grained access
3. Selective access
4. User privacy
5. Query privacy
6. Query and computation Integrity
7. Collaborative query execution with multiple providers SLA and Auditing
8. Multi-tenancy and Virtualization

V CONCLUSION & FUTURE SCOPE

In this paper present the review of data sharing and integrity over cloud computing. The major security issue in cloud computing is confidentiality availability and integrity. For the improvement of security parameter used various cryptography technique based on public and private cryptography. The message digests also improved the security strength of key encryption process. The policy of key encryption supported the data dynamics over the cloud computing environment. The process of data dynamics gives the concept of data auditing over cloud computing. In future used some standard key generation policy for the cloud data auditing.

REFERENCES:-

[1] Neetu Kishore and Seema Sharma "Secured Data Migration from Enterprise to Cloud Storage – Analytical Survey", BIJIT, 2016, Pp 965-968.

[2] Kajal Chachapara and Sunny Bhadlawala "Secure sharing with cryptography in cloud computing", IEEE, 2013, Pp 1-3.

[3] Preeti Garg and Dr. Vineet Sharma "An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function", IEEE, 2014, Pp 334-339.

[4] Syam Kumar Pasupuleti, Subramanian Ramalingam and Rajkumar Buyya "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications, 2016, Pp 12-22.

[5] Victor Chang, Yen-Hung Kuo and Muthu Ramachandran "Cloud Computing Adoption Framework – a security framework for business clouds", Elsevier, 2016, Pp 1-33.

[6] Alessio Botta, Walter de Donato, Valerio Persico and Antonio Pescape "Integration of Cloud Computing and

Internet of Things: a Survey", Journal of Future Generation Computer Systems, 2015, Pp 1-54.

[7] P.Vijaya Bharati and Dr. T.Sita Mahalakshmi "A Combinational Approach for securing the data in cloud storage using HMAC-SHA512 and Information Secured Algorithm (ISA)", International Journal of Applied Engineering Research, 2016, Pp 4081-4084.

[8] Vishal R. Pancholi and Dr. Bhadresh P. Patel "Enhancement of Cloud Computing Security with Secure Data Storage using AES", IJIRST, 2016, Pp 18-21.

[9] Wei-Fu Hsien, Chou-Chen Yang and Min-Shiang Hwang "A Survey of Public Auditing for Secure Data Storage in Cloud Computing", International Journal of Network Security, 2016, Pp 133-142.

[10] Kamlesh Kumar Rao and Sanjay Kumar Yadav "Implementation of Cloud storage Security Mechanism using Digital Signature", International Journal of Current Engineering and Technology, 2016, Pp 467-471.

[11] Pierangela Samarati and Sabrina De Capitani di Vimercati "Cloud Security: Issues and Concerns", Encyclopedia on Cloud Computing, 2016, Pp 1-14.

[12] S. R. Vijayalakshmi & S. Muruganand "Challenges in Integrating Wireless Sensor Network and Internet of Things for Environmental Monitoring", World Scientific News, 2016, Pp 8-15.