ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

Secure Cloud Storage Using AES Encryption

V.Surya[1], S.Ranichandra[2], R.Ranjani[3]

PG Scholar, Department of CS, Dhanalakshmi Srinivasan College of Arts & Science for Women, Perambalur, Tamil Nadu, India[1,3]

Assistant Professor Department of CS, Dhanalakshmi Srinivasan College of Arts & Science for Women, Perambalur, Tamil Nadu, India[2]

ABSTRACT: The cloud computing distributed resources are shared via network in open environment. Hence user can easily access their data from anywhere. At the same time there exist privacy and security issues due to many reasons. First one is dramatic development in network technologies. Another is increased demand for computing resources, which make many organizations to outsource their data storage. So there is a need for secure cloud storage service in public cloud environment where the provider is not a trusted one. This paper addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different security services like authentication, authorization and confidentiality along with monitoring in delay. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. The hosted services are offered to limited number of peoples, this minimizes the security concern. In public cloud, the infrastructure is owned and managed by cloud provider itself. Hence security and confidentiality of data is an important concern. In this proposed approach data is encrypted using AES and then uploaded on a cloud. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.

KEYWORDS: Network, Authentication, Authorization, Confidentiality, Security

I.INTRODUCTION

1 INTRODUCTION ABOUT THE PROJECT

The cloud computing model integrates several technological advancements such as virtualization, web services, and Service Level Agreement (SLA) management for enterprise application. Due to rapid development in technologies more and more service providers and customers moving towards cloud environment. Today military, government and commercial enterprise systems are using different cloud services to provide network connectivity and high service availability to the end users. Cloud providers offer their services in three fundamental models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Even though cloud computing has many advantages when compared with the traditional data storage mechanisms; security concern is a barrier for choosing cloud computing from the consumers view point. The researchers are done several studies related to security issues in cloud. Cloud infrastructure is mainly available in public and private mode. Private cloud is dedicated to a single customer or organization. The hosted services are offered to limited number of peoples, this minimizes the security concern. In public cloud, the infrastructure is owned and manasged by cloud provider itself. Hence security and confidentiality of data is an important concern. As the number of cloud users increases day by day, the Quality of Service (QoS) management is another important issue. QoS management in cloud computing environment refers to the activities in QoS specification such as evaluation, prediction, aggregation and control of resources to meet end-to-end user and application requirements. With the emergence in technologies a large number of organizations like IBM, Google, Yahoo, eBay etc., have already invested in cloud computing. Large number users share huge amount of data at high speeds from geographically dispersed locations. But in real cloud computing environment existing solutions are prone to failure and security compromise in many areas: computing performance, cloud reliability and information security. Present approaches are not sufficient to ensure data security for end users. The proposed approach provide a clear and concise view of delay within real cloud computing environments and

DOI: 10.15680/IJIRCCE.2018.0606031

inform cloud users about unauthorized access to their data through an SMS alert system. This paper discusses different research works done for management and monitoring of different QoS parameters in cloud. And also provides an abstract view of encryption techniques AES, DES and RSA.

II. SYSTEM STUDY

2.1 EXISTING SYSTEM

The data storage in cloud is similar to data stored in other storage devices but in remote locations. In cloud the user can access their data at anytime from anywhere. Three aspects of information security have to consider when using cloud services: confidentiality, integrity and availability. Public cloud infrastructure provide scalable and on demand data storage. This avoids the burden of creation and maintenance of private infrastructure for data storage. The customers get several benefits like reliability, availability with minimum cost and effort. But there exist some security and privacy risks. One important problem among them is confidentiality of customer data. One common solution to maintain data confidentiality is encryption. To ensure effectiveness of encryption there must use efficient encryption algorithm. In cloud computing environment where large amounts of data transmission, storage and handling occur, hence also need to consider processing speed as well as computational efficiency of encryption algorithm. In this case symmetric encryption algorithm is more suitable than asymmetric encryption algorithm.

Cloud computing security (sometimes referred to simply as “cloud security”) is an evolving sub domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There are several security issues exist within cloud computing. Selection of cloud vendors, users should ask about seven safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. The encryption algorithms mainly categorized into two: Symmetric and Asymmetric key encryptions. In symmetric key encryption single secret key is used for both encryption and decryption. In asymmetric key, encryption is performed using public key and decryption using secret key.
AES and Data Encryption Standard (DES) are two symmetric key encryption methods. Rivest-Shamir-Adleman (RSA) is example for asymmetric key encryption.

DES: The algorithm also referred as Data Encryption Algorithm (DEA). For DES data are encrypted in 64 bits blocks using 56 bit key. This algorithm transform 64 bit into a 64 bit output through a series of steps. The same steps and key is used for decryption also. In the initial step the 64 bit plain text passes through an initial permutation. Next phase consist of 16 rounds of both permutation and substitution functions. Last round consist of 64 bit output: the left and right half of the output is swapped, this will generate the pre-output. In the last step reverse of initial permutation is applied to the pre output, which produces 64 bit cipher text. DES finally and definitively proved insecure. According to them less than three days needed for breaking DES encryption. Fortunately there are a number of alternatives to DES like AES, Triple DES. DES is more vulnerable to brute force attack because of its short key length (56 bit).

RSA: Ron Rivest, Adi Shamir and Len Adleman at MIT published Rivest-Shamir-Adleman scheme in 1978. RSA is a block cipher. In RSA the plaintext and cipher text are integers between 0 and n-1. The typical size of n is 1024 bit.
DISADVANTAGES:

Less confidentiality and reliability of users data. DES encryption was performed in existing data security that will easily exploited by attacker.

2.2 PROPOSED SYSTEM

The proposed system built on a prototype of an online file processing application. One important application of this system is secure sharing of confidential data like medical record, personal information, financial information etc. Suppose a user wants to access our application for uploading their confidential data, she/he must register with their valid email id and mobile number with our system. The username and password for their account is user defined and not system defined. After successful registration they can login as a user. Then user can upload the confidential file through file upload module. Before uploading file to cloud, the user gets a window for encrypting their file as individual blocks. Then click the save button after setting a secret file ID for future accessing and sharing. The file will upload to the server database. In the case of medical record, user can share record with their doctor at anytime from anywhere, there is no need for keeping their files with them always as hard copy or soft copy. Only need is to remember their secret file ID. The file ID may be numbers, alphanumeric characters or special characters anything as user wish or they can use a combination of these as file ID. There is no limitation for length of file id. The user can view time taken for uploading their file. The proposed model used 128 bit AES encryption. The encryption consists of 10 rounds for 128-bit keys. In this model, the file was split into different blocks depending on file size. Then individual blocks are encrypted separately. After block wise encryption each block uploaded to cloud at different locations with file id and block id. If anybody like cloud provider, try to access a file directly from the server, they can't get whole data, since it stored at different locations and also in encrypted form. Hence the person who knows secret file id can retrieves data. The proposed system provides an online editing facility, i.e. user can edit their data and then uploaded on to cloud without downloading to their system. Only the actual user can use this facility while others can only view data. User authentication is performed through password verification. Each user has a unique user id and password for their account. During registration user set his/her own user id and password by which they can access their account for uploading their text files. When uploading file, each user have a unique file id for future access to their data. If user enters correct user name and password he/she get access to their account. Otherwise error message will be generated. Authorization is the process of verifying user's privilege to access something. In the proposed system, during unauthorized access to a particular file an SMS alert system is used to inform actual owner. Each file uploaded in cloud has a unique file id. Authorized users can use this ID for downloading and editing their uploaded data. If somebody tries to access another person's file, an alert SMS will send to the actual owner's mobile number which he/she provided during the time of registration.

ADVANTAGES:

The proposed system provides an online editing facility. Provide high security because files are stored in different blocks. Increase data confidentiality.

III. PROJECT DESCRIPTION

3.1 MODULES

1. Data Owner Registration:

Data Owner has a unique account. Hence, each data owner has to register initially before them accessing the cloud system. The registration is done by the data owner only once to create an account with username and password. Then she/he can login into the system from anywhere using the username and password and can also upload/download files through file upload and download module.

2. Cloud Access Provider:

A cloud service provider is a third-party offering a cloud-based platform, infrastructure, applications or storage services. It will provide storage service to data owner after the request was getting from data owner. Cloud Service Provider (CSP) is accepts the data owners request and sends cloud access permission to the data owner.

3. Uploading/Downloading:

Data owner can login from anywhere using her/his username and password and upload file, using their own file key. And later she/he can download the file using the same key. When uploading the file the content will encrypted using AES encryption before saved in to the database.

4. Data security:

128 bit AES encryption is used for provide security to the user uploaded data. AES is a fast symmetric encryption algorithm. So the chance for attack and uploading time are reduced. If there occur any unauthorized access an SMS alert will send to the authorized user.

5. Cloud Users:

Cloud users are the users who access the data from cloud server. Cloud users should register their details to the cloud for get permission to access the data from cloud. Data owner accepts the request from users, then share the specific key to access the data. Data users get key from owner then access the data on cloud.

6. Authorization Verification:

Authorization is the process of verifying user's privilege to access something. In the proposed system, during unauthorized access to a particular file an SMS alert system is used to inform actual owner. Each file uploaded in cloud has a unique file id. Authorized users can use this ID for downloading and editing their uploaded data. If somebody tries to access another person's file, an alert SMS will send to the actual owner's mobile number which he/she provided during the time of registration.

IV. CONCLUSION

CONCLUSION

Cloud computing proposed a new method for securing cloud data in real environment. 128 bit AES encryption is used for providing confidentiality, authenticity and access control. Then performance of proposed approach was analyzed based on delay. From this analysis we observed that there is drastic increase in delay with increase in file size. In the proposed system, during unauthorized access to a particular file an SMS alert system is used to inform actual owner. Each file uploaded in cloud has a unique file id. Authorized users can use this ID for downloading and editing their uploaded data. If somebody tries to access another person's file, an alert SMS will send to the actual owner's mobile number which he/she provided during the time of registration.

FUTURE ENHANCEMENT

In Future of this project pairing based key matching algorithm is to implement to check authority of the user.

ACKNOWLEDGEMENT

The author deeply indebted to honorable SHRI A.SRINIVASAN(Founder Chairman), SHRI P.NEELRAJ(Secretary) Dhanalakshmi Srinivasan Group of Institutions, Perambalur for giving me opportunity to work and avail the facilities of the College Campus. The author heartfelt and sincere thanks to Principal Dr.ARUNA DINAKARAN, Vice Principal Prof.S.H.AFROZE, HoD Mrs.V.VANEESWARI, (Dept. of CS) Project Guide Mrs.S.RANICHANDRA, (Dept. of CS) of Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur.The author also thanks to parents, Family Members, Friends, Relatives for their support, freedom and motivation.

REFERENCES

[1] Giuseppe Ateniese, "Provable Data Possession at Untrusted Stores", Proc. of ACM Conference on Computer and Comm. Security (CCS),2007.
[2] Ari Juels and Burton S.Kaliski Jr, "Pors: Proofs of Retrievability for Large Files", Proc. Of ACM Conference on Computer and Comm. Security (CCS), pp. 584-597, 2007.
[3] Hovav Shacham and Brent Waters, "Compact Proofs of Retrievability," International Conf. on Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 90-107, 2008.
[4] Giuseppe Ateniese, "Scalable and Efficient Provable Data Possession", International Conf. on Security and Privacy in Comm. Networks (SecureComm), 2008.
[5] C. Chris Erway, Alptekin Kupcu, Charalampos Papamanthou, Roberto Tamassia, "Dynamic Provable Data Possession", ACM International Conf. on Computer and Comm. Security (CCS),2009.
[6] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 –859, 2011.
[7] Cong Wang, S. M. Chow, Qian Wang, Kui Ren and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transaction on Computers, Vol. 62, no. 2 , 2013.
[8] Sarah Shaikh, Deepali Vora, "Review of Privacy Preserving Auditing Techniques", International Journal of Computer Applications (0975- 887) , Volume 145 – No.13, July 2016.
[9] T S Khatri, G B Jethava "Improving Dynamic Data Integrity Verification in Cloud Computing", 4th IEEE ICCCNT 2013.
[10] S. V. Baghel, D.P. Theng " A Survey for Secure Communication of Cloud Third Party Authenticator ", 2nd International Conference on Electronics and Communication Systems, IEEE ICECS '2015.

BIOGRAPHY

1. **Mrs.V.SURYA** is presently pursuing M.Sc., Final year the Department of Computer Science from Dhanalakshmi Srinivasan College of Arts and Science for Women,perambalur, Tamil Nadu India.

2. **Mrs. S.RANICHANDRA -** Received M.C.A, M.Phil Degree in Computer Science. She is currently working as Assistant Professor in Department of Computer Science in Dhanalakshmi Srinivasan College of Arts and Science

for Women, Perambalur Tamil Nadu, India. She has Published papers in various journals like Network Security and neutrals system.

3. **Ms.R.RANJANI** is presently pursuing M.Sc., Final year the Department of Computer Science from Dhanalakshmi Srinivasan College of Arts and Science for Women, perambalur,