Level-Based Data Security Model in Cloud Computing

Kanupriya, Meenakshi Sharma

Abstract: Cloud Computing has brought remarkable advancement in era of computing but still adoption of cloud now days become issue due to security. Security is big concern in cloud computing. Data owner feels that data is insecure hands and vulnerable to many threats. To tackle this problem model has been proposed which check data security at different levels i.e. at cloud service provider level, user level, third party level and network intruder level. Various cryptography techniques used for data encryption, message authentication code is generated for data integrity and role-based dual verification is performed for user authenticity. The proposed model is highly efficient and secure for keeping data at cloud with minimum overhead over data owner. This model also provides data confidentiality, availability, data integrity and cost effective for storing data at cloud without risk.

Index Terms— Cloud Computing, MAC, Security, Encryption.

I. INTRODUCTION

Cloud Computing is biggest innovation in today's world of computing. It is tremendously gaining attention in scientific and Information Technology sector. Raj Kumar Buyya et al. [1] conducted a study that computing will be forthcoming utility (after water, electricity, gas, and telephony). This computing utility will serve as the most elementary level of computing service that will be needed to fulfil daily needs. Basically, Cloud computing is anything whether it is storage, hardware, software or full virtualized machine accessing them from anywhere, anytime using internet. These storage, hardware or software which is delivered to user remotely are maintained and monitored by cloud service provider. Cloud provides elasticity for dynamic resource pooling, quality of on-demand self-service and cheapest as user is charged pay-per-use basis. In spite there are a lot of merits that influence user to adopt cloud but still there are significant obstacles which don't allow client to proceed towards it. The main stumbling block concern is data security at different levels. Client may range from an individual to big organization. Data Security at different levels concerns with two aspects: External level security and internal level security. External level security deals with data insecure against third party, cloud service provider or network intruder. Internal level security deals with authorized users or employee of an organization. Data Security concerns with sensitivity of data stored to different types of cloud environment.[6] This major issue is barrier to different range of people and barred them from adopting cloud. To resolve this problem related to sensitivity of data we propose a security model based on verification of data at different security level that i.e. cloud service provider level, network intruder level, user level or third party level. In this model, we deploy standard algorithms such as RSA, DSA, AES etc. to encrypt data before sourcing it to cloud and also made the scheme for dual authentication of users. The rest of paper is assembled as follows: Section II represent related model already proposed in the field of data security in cloud. Section III we discussed our proposed model and technique for data security and user authentication. Section IV analysed the security at different levels and perform comparative analysis of our model with existing security models. Section V represents productive Conclusion.

Manuscript published on 30 July 2014.
***Correspondence Author(s)**

Kanupriya, **Kanupriya**, is Pursuing M.Tech in Computer Science & Engineering at SSCET, Badhani, Punjab, India.
Meenakshi Sharma, is Working as Assoc. Prof. in Department of Computer Science & Engineering, SSCET, Badhani, Punjab, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. RELATED WORKS

There a lot work in carried out in in the field of data security. Many models and schemes has been proposed. Sood et.al [2] proposed approach to ensure data security in cloud computing. In this proposed approach key generation, encryption, indexing of data, user authentication and data integrity is performed by data owner itself. Unfortunately, there will be high overhead on data owner and hence time consuming too. Jing et.al [4] describes the security of data in cloud using hadoop framework. The proposed scheme focuses only on data encryption technique like DES or AES not on authorized user access. So, vulnerable to different attacks related to unauthorized access. Sharma et.al.[8] discussed different service model of cloud computing and highlights the key security issues, challenges and solution at different layers of cloud. Thilakanathan et.al [3] proposed scheme using proxy re-encryption for security of data. In this scheme data owner encrypt the data using his key piece then proxy encrypt the data using his key piece. Decryption is also carried in similar fashion. However, if proxy is fake then data becomes insecure. Jingwei et.al.[7] discussed efficient model for secure data sharing in cloud. The proposed model consists of user, authority, hybrid cloud and owner. The data is stored at private cloud and data shared is encrypted. Encryption technology used is keyword-based encryption. The keys are generated by authority and given to user group for encryption and decryption. The model has some issues like if authority is fake then data is insecure and also it is costly to use the model. Sood et.al [4] proposed the scheme to highly secure the data at cloud. They provided improved data security by using concept of hybrid cloud. In this scheme the sensitive data i.e. about 3%-5% is stored at private cloud and rest of the data at public cloud. This model is applicable to organisations whose sensitive data is about 3%-5%.

If the sensitive data increases then this model will prove to be expensive. The whitepapers [10] of many organisations describes three types of data security models in cloud. First model consists of key generation and encryption on data is performed by data owner itself. However this model results in high overhead for data owner. Second model describes encryption performed by data owner and key generation by cloud service provider. Unfortunately, cloud service provider is fake then data is insecure hands. Third model encryption and key generation is control by cloud service provider. If cloud service provider is fake then data is endangered. In cloud computing most prevailing issue is security due to which users fear to adopt cloud. Main concern is with uploaded data to cloud is secure or not. Keeping this concern model has been proposed which provide data security in cloud. It is highly efficient and secure model that can be used to upload data in cloud without fear.

III. Proposed Model

The Proposed model has been organized in such manner that data is secure during transfer as well as in cloud itself. The proposed model consists of four entities – data owner, user, cloud service provider and third party. The data is protected against network intruder, dishonest cloud service provider, suspicious third party and unauthorized user. The model is described as follows:

A. *Categorization*

In order to secure data encryption is technique used in proposed model. Encryption of data is carried according sensitivity of data. The data is classified as: Type0 and Type1.

Type0 – Data is not sensitive i.e. no need to encrypt data. Data is directly uploaded to cloud without encryption.

Type1 – Data is sensitive and need to encrypt data before uploading to cloud.

Type0 or Type1 depends on response of data owner.

B. *Data Encryption and Decryption*

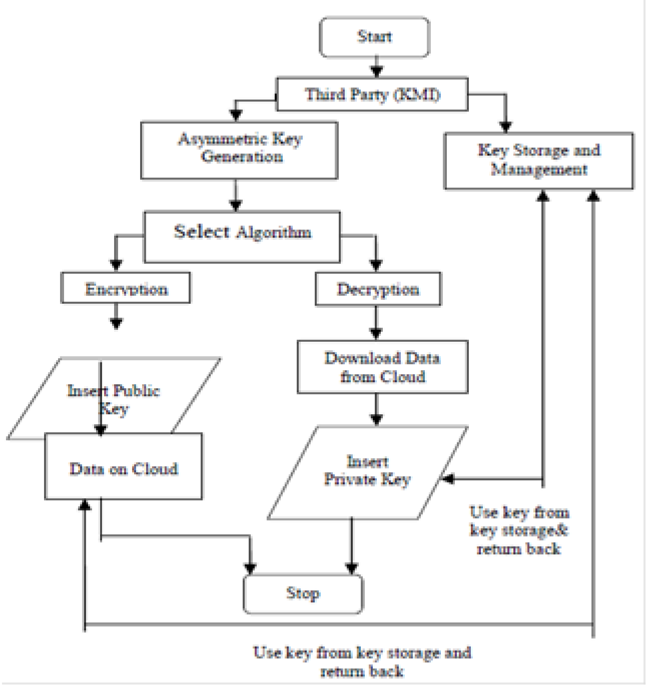

Fig. 1 Data Encryption and Decryption

Data Encryption and decryption is carried by three entities Third party which act as Key Management infrastructure. Main responsibility is to provide key management and key storage. Key storage includes key generation, protection and storage. Key management includes providing keys to authorized user i.e. after verification of user proving keys. Keys are encrypted with passcode. In this model, it is assumed that third party do not know about cloud service provider. The standard algorithm like RSA, AES etc. used for encryption and decryption.[9]

C. *Data Integrity*

In order to check the integrity of data i.e. the data has been tampered or not during transit over network Message Authentication Code (MAC) is calculated. In this model after encryption is done then MAC is calculated over encrypted data and attached with the encrypted data during uploading to cloud. When user or data owner require data they download data from cloud and check data integrity by calculating MAC. Data owner or user Matches the MAC attach with MAC calculated. Standard MD5 message-digest algorithm is used for data integrity.

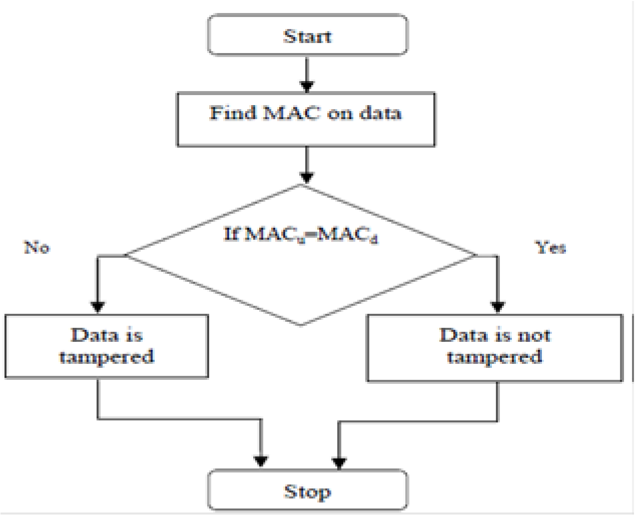

Fig. 2 Data Integrity

D. *Role Based Dual User Authentication*

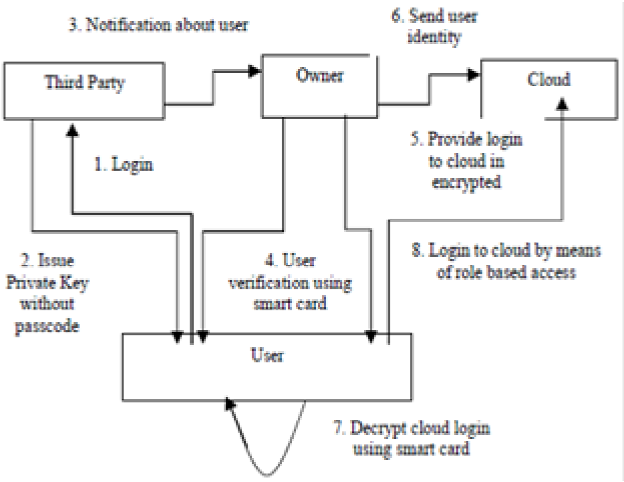
3. Notification about user
6. Send user identity
Third Party
Owner
Cloud
1. Login
5. Provide login to cloud in encrypted
2. Issue Private Key without passcode
4. User verification using smart card
8. Login to cloud by means of role based access
User
7. Decrypt cloud login using smart card

Fig. 3 Role-Based Dual Authentication

For user authentication dual verification is carried out by third party and further verified by data owner. Owner gives list of authorized user with login id and password to third party. Third party makes the database for user authentication. When user login with user id and password the third party verifies the user by checking its database. If user is an authorized user then third party issues private key without passcode and also notify data owner about user. Now further verification performed by data owner. Data owner verify user using smartcard if verified then owner provide cloud login id, password and passcode of private key in encrypted format. This encrypted data is decrypted using smartcard. User sends the identity of user to cloud so that cloud service provider allow user to login to cloud to access data. Now user login to cloud to access data. There is role based access to data i.e. user can update, read or delete etc. according to data owner wish.

IV. SECURITY ANALYSIS

Proposed model has been organized so that it give throughout data security in cloud computing at different levels. The different levels are: user level, cloud service provider level, third party level and network intruder level. Data is protected against all level

A. Security at User Level

Role based Dual verification of user is carried out in proposed model. Data is protected against unauthorized access. When user needs data it has to undergo dual verification from third party as well as data owner itself. Once the user verified by both the parties, authorized user can access the data by login to cloud. Access to data is role based i.e. authorized user can read, update or delete data according to data owner wish. Data owner sets the permissions on data for their user. Data is protected from unauthorized access.

B. Security at Cloud Service Provider

Encrypted data is uploaded over cloud in order to protect data against cloud service provider. Thus even if cloud service provider is fake data is secured.

C. Security at Third Party Level

In proposed model third party act as Key Management Infrastructure. At this level data is verified to be secured against third party. In proposed model it is assumed that third party do not know about cloud service provider. Even if third party knows about cloud service provider, login id and password of authorized user then also third party cannot get cloud login id and password. During user verification by data owner third party will need smart card that was given to authorized user by organization for user authentication. So data is secured even if third party is untrusted.

D. Security at Network Intruder Level

Network intruder hijack the session and redirect all the traffic towards itself. Still data is secure as data is in encrypted form and remains un-useful to intruder.

E. Parameters

There are some parameters which make this model attractive to adopt are Confidentiality, Availability, Integrity, Overhead, Authorization and Dual Authentication. As the data remain encrypted throughout the model so confidentiality of data is retained during transit as well as at rest. Data in cloud is available 24*7 as per service level agreement. In proposed model data security is divided equally among third party and data owner itself so less overhead on data owner. Role based access to data and dual verification through smartcard make access to data highly secure. Message authenticated code is generated for checking data integrity. All these factors of proposed model make data highly secure at cloud and adoption to cloud easy for users.

V. CONCLUSION

Cloud computing has brought remarkable change in world of computing. Cloud comes with lots of benefits but still users hesitate to adopt it. Main reason or fear in user mind is regarding security whether their data is in insecure hands or is it safe to upload their sensitive data over cloud. Most prevailing issue in world of computing is security. To solve this problem of data security a model has been proposed. In this model data security is checked where there is possibility of data threat. Data security is checked at different levels that are:- user level, cloud service provider level, network intruder level as well as at cloud service provider level. The outcome of this proposed model is that data is kept secure at cloud. This model provides data confidentiality, rapid availability on demand, data Integrity and minimum overhead to data owner, cost effective and efficient.

REFERENCES

1. Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi, Mastering Cloud Computing Foundations and Applications Programming. Morgan Kaufmann, USA.
2. Sandeep K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing", Submitted to Journal of Network and Computer Applications, Elsevier Ltd, 2012.
3. Danan Thilakanatha, Shiping Chen,Surya Nepal, Rafael A. Calvo and Leila Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud", Elsevier Ltd, 2013.
4. Huang Jing, LI Renfa, and Tang Zhuo, "The Research of the Data Security for Cloud Disk Based on the Hadoop Framework" Fourth International Conference on Intelligent Control and Information Processing (ICICIP), IEEE June 9 – 11, 2013, Beijing, China.
5. Sandeep K. Sood, "A Highly Secure Hybrid Security model for Data Security at Cloud ", Submitted to Security and Communication Networks, John Wiley and Sons (Interscience),Special Issue on Trust and Security in Cloud Computing, 2012.
6. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing" Journal of Internet Services and Applications ,Springer 2013.
7. Jingwei Li, Jin Li, Zheli Liu and Chunfu Jia "Enabling efficient and secure data sharing in cloud computing" Concurrency Computat.:Pract Exper.,John Wiley & Sons, Ltd.,2013.
8. Pardeep Sharma, Sandeep K. Sood, SumeetKaur, "Cloud Implementation Issues and What to Compute on Cloud", International Journal of Advances in Computer Networks and its Security, vol.1, no. 1, pp. 130-135, 2011.
9. Marten van Dijk and Ari Juels,"On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing".
10. Amazon Web Services.: "Encrypting Data at Rest in AWS", https://aws.amazon.com/whitepapers.
11. NarendraChandel, Sanjay Mishra, Neetesh Gupta and Amit Sinhal "Creation of Secure Cloud Environment using RC6", International Conference on Intelligent Systems and Signal Processing (ISSP), IEEE, 2013.

12. Swetha Reddy Lenkala, Sachin Shetty and Kaiqi Xiong, "Security Risk Assessment of Cloud Carrier", International Symposium on Cluster, Cloud, and Grid Computing, IEEE/ACM, 2013.
13. Dimitrios Zissis and Dimitrios Lekkas "Addressing cloud computing security issues", Elsevier, 2010.
14. Chirag Modi , Dhiren Patel, Bhavesh Borisaniya, Avi Patel and Muttukrishnan Rajara, A survey on security issues and solutions at different layers of Cloud computing", Springer, 2012.
15. Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser, "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing: Advances, Systems and Applications, Springer 2012.

AUTHOR PROFILE

Kanupriya, is pursuing M.Tech in Computer Science & Engineering at SSCET, Badhani, Punjab, India under Punjab Technical University, Jalandhar. Her ongoing research area is Security at cloud and her areas of interest are Cloud computing and network security.

Meenakshi Sharma, is working as Associate Professor in Department of Computer Science & Engineering, SSCET, Badhani, Punjab, India. She has more than 16 years of teaching experience. Her areas of interest are Parallel Computing, Cloud Computing, and Network security.