International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Multiple Attribute Based Data Security in Cloud Computing – A Review

Nitica Bir[1], Maninder Kaur[2]

[1]M.Tech Scholar, Doaba Institute of Engineering and Technology, PTU, Jalandhar, India

[2]Assistant Professor, Doaba Institute of Engineering and Technology, PTU, Jalandhar, India

Abstract: ***In this new era, receptive data is stored and shared on internet. Cloud computing is one of the upcoming technologies used for bulk data and its storage. It is revolutionary computer paradigm which enables flexible, on demand and low cost usage of computing resources. Cloud storage provides virtualized pools of storage and people buy or lease storage capacity from them. For remote data storage, data security and privacy are critical issues. A secure user enforced data access control mechanism must be provided before cloud users have liberty to outsource sensitive data to cloud for storage. To avoid unauthorized access, data should be encrypted before outsourcing. To deal with security problems, various schemes based on attribute- based encryption have been proposed. Attribute is a way of public key encryption in which secret key of user and cipher text are dependent. The decryption of cipher text is only the set of attributes of user key matching the attributes of cipher text. Attribute-based encryption also enables access control over encrypted data using access policies and ascribed attributes. Encrypter has full control over access rights, providing feasible key management. In role- based system, policies can be generated and based in that policies, encryption can be done. Generation of access key is based on access policies assigned to each user along with attributes. The data stored in cloud is encrypted and decrypted using a key generated based in access permissions assigned to data attributes of owner who share their data with high security and integrity using policy based multiple attribute based encryption(MABE).***

Keywords: Cloud computing, Storage in cloud. Access key, Access control, Security, MABE, Attribute-based encryption

1. Introduction

When cloud computing is a new and fast growing technology for data storing and computing techniques. It is general term for anything that involves delivering hosted services, scalable services like data sharing; accessing etc. over the web on user demand basis. It uses web and central remote servers to maintain data and application. Data security is a major obstacle in way of cloud computing. So, confidentiality, integrity and access of data should be guaranteed. Data owners can't even trust on users as they may be malicious. The servers might illegally inspect user‟s data and access sensitive information. On the other hand, unauthorized user may also be able to intercept someone's data. Moreover, personal information (defined by user's attribute) is at risk because one's identity is authenticated according to his information .Many schemes are given to ensure these security requirements but they are suffering from collusion attacks of malicious users and cloud service providers(CSP).To address these issues, we propose a scheme multiple attribute based encryption. In this scheme, there are basically three entities: data owner, cloud service provider and users. Users are divided in groups on some basis such as location, project and department and corresponding to each group there is single key for encryption and decryption of data. Sahai and Waters proposed Attribute-based encryption (ABE) where decryptor could decrypt the message if and only if his identity is exactly the same as what specified by encryptor. The decryption keys are disclosed only to authorized users. Key-policy attribute based encryption (KP-ABE) and cipher text policy ABE(CP-ABE) are proposed by Goyal et al. and Bethencourt et al. respectively. In KP-ABE, cipher text is associated with set of attributes which partially represent the cipher text‟s encryption policy. A user can decrypt cipher text if and only if access tree in his private key is satisfied by attributes in cipher text. In CP-ABE, cipher text are created with an access structure, which specifies the encryption policy, private keys are generated according to user's attributes. A user can decrypt the cipher text if and only if his attributes in private key satisfy the access tree specified in cipher text. By doing so, encrypter holds ultimate authority about encryption policy. A crucial property of ABE system is that they resist collusion attacks. It is achieved by binding together the attribute secret keys of specific user with a random number so that only those attributes can be used for decryption which contains the same random values as the others. As a result private keys must be issued by one central authority (CA) that would need to be in a position to verify all the attributes or credentials it issued for each user in the system. The data owner may want to set some restrictions to clients who are trying to access the data. Multi owner/Role based system is a model for sharing and accessing business data of large Organization which allows owners to create, manage and control their information/data in cloud. Cloud storage permits large number of users having different roles and access permissions to share and store their data.

2. Literature Review

The literature review includes enunciation of relationships between research field and literature. The form of literature review may change with different type of studies but basic purpose remains same.

[2014] Subham Kumar Gupta, Seema Rawat, Praveen Kumar ,A Novel Based Security Architecture of Cloud Computing‟: In this paper, the basic dilemma of cloud computing security is inspected. Authors have also proposed a survey of various models for cloud security. To ensure the data security in the cloud, we suggest an efficient, accessible

and adaptable cryptography based scheme. In-depth security and enactment inspection proved the proposed scheme as greatly efficient and robust against spiteful data alteration outbreak.

[2014] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma and Sundaram Vats „Threshold Cryptography Based Data Security in Cloud Computing": Authors have proposed a scheme that uses threshold cryptography in which data owner divides users in groups and gives single key to each user group for decryption of data and, each user in the group shares parts of the key. In this paper, authors use capability list to control the access. This scheme not only provides the strong data confidentiality but also reduces the number of keys.

[2014] Sushmita et.al. have proposed a decentralized access control with anonymous authentication of data stored in clouds. Authors proposed a new decentralized access control scheme for secure data storage in clouds, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user"s identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

[2014] Bharathy, S. Divya have developed securing data stored in clouds using privacy preserving authenticated access control. Authors proposed a privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds, which are centralized. We also provide options for file recovery. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks. User revocation and access control policies highly contributes to avoid abuse of cloud services and shared technology issues.

[2013] Lee, Keunwang, and Haeseok Oh. et al. have conducted a research project on access control method by user authority using two-factor authentication. The important information of individuals and businesses is leaked or processed by outside attacks or personal mistakes, thus misused, and thereby considerable damage is occurring. For this reason, the necessity of how to effectively manage personal and corporate information is emerging. This study intends to suggest a method that can protect servers and media information, which requires security. The access control method suggested here uses a way that grants users authority by grade and authenticates users through Two-Factor Authentication method.

[2013] Wazan, Ahmad Samer and Gregory Blanc have worked on attribute-based mining process for the organization-based access control model. Authors have propose to bridge the gap between the theory of access control models and the reality of organizations by defining an attribute-based mining process that deduce the abstract concepts starting from the attribute level. Additionally, the attributes allow us to semantically enrich the obtained results. We have selected the Organization-Based Access Control (OrBAC) model as the abstraction objective of our study.

[2012] Kabir, M.E. have worked on a role-involved purpose-based access control model. The structure of a CPAC model is defined and investigated. Access purpose is verified in a dynamic behavior, based on user attributes, context attributes, and authorization policies. Intended purposes are dynamically associated with the requested data object during the access decision. An algorithm is developed to achieve the compliance computation between access purposes and intended purposes and is illustrated with role-based access control (RBAC). Access purpose authorization and authentication in the model are studied with the hierarchical purpose structure. The model separates authorization of access purpose from access decision that improves the flexibility of private data control.

3. Problem Formulation

Cloud computing is considered as the future of IT organizations. In weigh against to conventional solutions where all type of computing services are controlled through any type of personnel controls, it transfers all computing resources to the centralized large data centers, so users can enjoy services in a large scale on demand. Cloud Computing do not keep data on the user"s system, so there is a need of data security. In order to retain confidentiality of data against un-trusted cloud service providers, authors have also proposed a survey of various models for cloud security. To ensure the data security in the cloud, an efficient, accessible and adaptable cryptography based scheme has been suggested. In-depth security and enactment inspection proved the proposed scheme as greatly efficient and robust against spiteful data alteration outbreak.

In previous model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. This scheme can be as a advancement of cipher text-policy attribute- set-based encryption (CP- ASBE) scheme. The problem has been found in this work; of less security because of single attribute policy has been used. The second problem is related to time concern and the last one is data privacy.

4. Proposed Model

In this research, a cloud data security model for the cloud storage using third party auditors which will be implemented by combining various techniques together to achieve the data security and data privacy goal has been proposed. The

techniques included in the combination would be Encryption of data, key exchange, dividing the user groups. The proposed model has been divided into three major components: Encryption of Data, Key exchange, divining the user groups. Encryption will store the data in cipher form, with key exchange user can decrypt the data and divining the user into groups means each group has access to relevant data. This means, if a hacker will attack and download the data, he will have to work hard a lot to access the data caused by the mathematical computations to generate the key and decrypt the data? Then the data encryption will be used to create a completely unreadable and hashed data. A fast and robust variant of data encryption will be used for the encryption module. To solve the issue of data privacy, every user will be assigned a right to access the file. The combine scheme will be called as PCP-MABE (Pipeline Cypher Policy- Multiple Attribute Based Encryption).

5. Conclusion

At first stage, a detailed literature study would be conducted on the existing cloud storage security solutions. Literature study will lead towards refining the structure of the proposed cloud security solution design. Afterwards, the proposed solution will be implemented in MATLAB simulator in three phases: In first Phase Using third party auditors will perform authentication using the credentials. In second Phase, Data Encryption will be done. In third phase multiple attributes will be set for the data. Divide the data into smaller segments using pipeline concepts. Generate a key to encrypt the data. Encrypt the data and store the data. In Last phase, User can access the data according to assigned role by data owner. After receiving the data user decrypt the data with shared key and by applying the attributes.

References

[1] Bharathy, S. Divya, and T. Ramesh. "Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control." (2014).
[2] Kabir, M.E., Wang, H., and Bertino, E. (2012), “A Role-involved Purpose-based Access Control Model”, Information Systems Frontiers, 14(3), 809-822
[3] Krikelas, Ilias, IoannisXydas, and Pierre-François Bonnefoi. "Graphical User Authentication in Mobile Device using the web RGB color palette." In BCI (Local), p. 65. 2013.
[4] Lee, Keunwang, and Haeseok Oh. "Research on access control method by user authority using two-factor authentication." In Proceedings of the 1st International Conference on Convergence and It‟s Applicatio (ICCA‟013), vol. 24, pp. 172-175. 2013.
[5] Malik, Jyoti, DhirajGirdhar, RatnaDahiya, and G. Sainarayanan. "Multifactor Authentication Using a QR Code and a One-Time Password." Journal of Information Processing Systems 10, no. 3 (2014).
[6] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "Adopting provenance-based access control in OpenStack cloud IaaS." In Network and System Security, pp. 15-27. Springer International Publishing, 2014.
[7] Nag, Abhijit Kumar, DipankarDasgupta, and Kalyanmoy Deb. "An Adaptive Approach for Active Multi-Factor Authentication." In 9th Annual Symposium on Information Assurance (ASIA‟14), p. 39. 2014.
[8] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "Adopting provenance-based access control in OpenStack cloud IaaS." In Network and System Security, pp. 15-27. Springer International Publishing, 2014
[9] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "A provenance-based access control model for dynamic separation of duties." In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, pp. 247-256. IEEE, 2013.
[10] Ruj, Sushmita, Milos Stojmenovic, and AmiyaNayak. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds." Parallel and Distributed Systems, IEEE Transactions on 25, no. 2 (2014): 384-394.
[11] Subham Kumar Gupta, SeemaRawat, Praveen Kumar “*A NOVEL BASED SECURITY* ARCHITECTURE OF CLOUD COMPUTING ” 978-1-4799-6896-1/14/$31.00 ©2014 IEEE
[12] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma and Sundaram Vats “Threshold Cryptography *Based Data Security in Cloud Computing*” Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on 978-1-4799-6023-1/15 $31.00 © 2015 IEEE DOI 10.1109/CICT.2015.149
[13] Wazan, Ahmad Samer, Gregory Blanc, Hervé Debar, and Joaquin Garcia-Alfaro. "Attribute-based Mining Process for the Organization-Based Access Control Model." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 421-430. IEEE, 2013.