International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

A Comparative Study on Privacy Preserving Schemes based on Encryption Proxy and Cloud Mask

Umar Khalid Farooqui[1], Prof. P.K. Bharti[2], Prof. (Dr) Mohammad Hussain[3], Dr. Rajiv Pandey[4]
[1, 2, 3, 4]*Research Scholar MUIT, Department of Computer Science & Engineering MUIT, Department of Computer Science & Engineering M.G Institute of Management &Technology, AIIT Amity University Lucknow*

Abstract: Cloud Computing gains popularity day by day and the data generated on internet is multiplying at a very high pace but this rapid growth of data may leads severe security and privacy concern specially data which is outsourced(whether on rest or transmit)needs protection, In this regard various researchers proposed different schemes and models based on Cryptographic mechanism, proxy based service models.
In this paper we made an attempt to present a comparative study on two such popular privacy preservation schemes, namely – Encryption Proxy and Cloud Masked model for secure data storage on cloud
Keywords: Encryption Proxy, cloud Mask, data storage, cloud, Access Control.

I. INTRODUCTION

"Cloud computing is a resources provisioning system which delivers its service on demand over Internet"[8] . Cloud computing is provisioning any kind of computing resources like data, information, file, any other resources to its subscriber(s) on their demand over the Internet.
Clouds computing is a recent technology used to represent a different way to architect and remotely manage computing resources; it is sharing resources/information as-a –service using internet. Cloud Computing could be thought as a platform and type of application[9].
Cloud computing offers a new road map for utilizing as well as delivering of computing resources. The provision is based on the Internet which are dynamically scalable and most of the time these are virtualized resources.
"Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements"[8].
Cloud users can utilize the services of cloud in a pay-per-use basis and they save noticeable upfront cost of building their own rigid infrastructure. The name and fame of cloud multiplies day by day however the customer of cloud is always keen to know about the protection of their sensitive data inside of cloud.
Also the local administrator as well as CSP will definitely not learn about user data even while performing intended operations.[1]
The data which is outsourced whether on transmit or rest needed protection from unauthorized access and if cloud provider is not ensuring this, the trust of cloud user may affect badly [12].Therefore privacy preservation is a hot research area in cloud computing.
"The amount of data produces and managed by cloud is highly appreciated day by day with the advent of next generation technologies"[13]. Google, Amazon, IBM are some well known provides for storage services of cloud. But outsourcing of data clearly attracts security issues . The cloud service provider is responsible to ensure security to the outsourced data and promise the reliable services to its client. The data storage must insure confidentiality ,integrity and availability. The cloud service that provide storage as a service must ensure that data not modified or accessed by unknown/unauthorized person[14].
For Ensuring privacy of the outsourced data many researchers present schemes and models based on Access Control Policies, cryptography techniques. Some of which are discussed here.

II. PRIVACY PRSERVATION SCHEMES

Ulrich Greveler et al. Proposed a cloud data storage architecture that restrict cloud administrator and local administrator to learn about outsourced database content[10].They use machine readable rights expression to limit the user of data base.
In this architecture they introduced new role of "rights editor" which defines once while application launche. They introduced a secure privacy preserving cloud data storage architecture and the main focus is on SaaS.

In this scheme the cloud server/administrator is prevented from learning content in the outsourced database because of using encryption. However still there is a need for finding ways to restrict employees using cloud application to learn more than their privileges..

Greveler et.al main contribution is a system architecture that allows a flexible and adequate "Access Restriction Writing". The system can resist from both external and internal attackers.

In this system all data are stored encrypted, the backup of database is performed regularly by the cloud service they automate. The backup procedure for encryption proxies is designed while establishing system integrity first then exchanging the decryption keys over a secure channel also all session keys are TPM sealed for enhancing security[7].

A. System Architecture Detail

The productive database is stored on the cloud and consists of following three parts.

1) Data Management (Cloud itself plays this role)
2) Encryption Proxy (Intermediary between cloud and user)
3) User Interface(With which user interacts with the system)

The content of productive database is encrypted also for load balancing clients are not bound to a single encryption proxy. The productive database includes a meta data table where information of each user's transactions are stored.

The encryption proxy is the key part of the system , it provides user access to the (unencrypted) data. The encryption proxy acts as an intermediary between cloud and user. The encryption proxy comprises of following parts:

4) Web Interface: It sends a request together with session ID to the User Client over a secure channel.
5) User Client: The UC afterward creates a XML-RPC request to the User Engine. This XML RPC consist of the credentials and the request from web interface. To secure the request it's all parts are encrypted.
6) User Engine: It receives request from UC and checks for the signature, if the signature is genuine the system will decrypt the user credentials the UE next check the credentials and append the User Id and Group Id to encrypted request and forward it to Rule Engine.
7) Rule Engine: The RE looks up the access control file for allowed function related to UID(or GID), when a function P is found, the RE also ascertained the use file f. The RE search in the secure storage for the used database d and the decryption key Kf .Next RE calculates the computation request for database p(f) and sends the request to the cloud database.

B. Major Benefits of the Model

1) This is an attempt to make cloud data self intelligent.
2) They use TPM to seal all the session keys, TPM sealing function binds data to a secure state[7].
3) This system provides no login shell.
4) Here decryption is only on demand and reduce time consumption while the system is booting up.
5) They use Access Control Language such as XACML(Extensible Access Control Markup Language) for the rule engineRE ,XACML enables us to have complex access rights together with XML signature.
6) Here we can specify rules to limit the daily request for an employee to access the productive database and prevent download of the whole database.
7) Only the content of secure storage is changeable within the encryption proxy.

C. Limitations

1) This leads to performance overheads as each time there is a need for recalculation or redefining rules for the rule engine.
2) In case of huge number of upcoming request it gives confusion.
3) At any time entire control is on Encryption Proxy.
4) Compromising the proxy leads the system failure.
5) The creation of complex machine readable access rights to the decryption keys become a challenging problem.
6) XML based rights expression is complicated and obscure.

M. Nabeel et.al, identifies challenges in securing DaaS Model and proposed a system called "clod mask" for securing organizational data using fine grained and flexible access control for shared data hosted in the cloud[2]. Generally Storage as a service(SaaS) provide a virtual storage while Data as a Service(DaaS) provide a higher level interface to store and query data on a

data structure, and in cloud data services, data privacy and security are major concerns, thus an important requirement is to support fine grained access control, based on policies specified in a expressive access control language , over encrypted data hosted in cloud.

D. Cloud Mask- Architecture

They assume organizational data are grouped into documents each data item in a document is called subdocument.

Cloud Mask consist of following components

1) *Document Manager (DM):* It is an in house entity that manages subscription and performs policy based encryption of documents. Some part of computations performed by DM can be moved to a cloud infrastructure, such as Amazone EC2 we need to make sure that the actual keys are not exposed to the cloud.
2) *Cloud Data Service (CDS) :* It is a third party cloud service for hosting the encrypted documents, the CDS may work under SaaS or DaaS model.
3) *Users (Usrs):* Usrs are the employees of the organization they register with the DM and retrieve documents from the CDS.
4) *Identity Providers (IdPs):* IdPs are the independent entities that issue certified identity tokens i,e., commitments of identity attributes to Usrs. Nabeel et. al, claim that this system is a promising step to minimize any identity theft lead attacks by insiders/outsiders. Since the DM and CDS do not learn identity attributes of Usrs.

Cloud Mask is satisfying following security and privacy requirements.

5) The DM and CDS do not learn the identity attribute of Usrs.
6) The CDS does not learn the content of subdocuments.
7) Attribute based access control is enforced for the subdocuments.
8) The CDS provides a mechanism to restrict the access to subdocuments only to authorized Usrs without learning their Identity attributes. Cloud Mask is based on following building blocks
9) Oblivious Commitment Based Envelope (OCBE) protocol.
10) Broadcast group key management (BGKM) Schemes.

OCBE protocol are proposed by Li and Li[6], they provide a way to obliviously deliver a message to the Usrs who satisfy certain conditions. The DM and Usrs engage in OCBE protocols for the Usrs to obtain secrets for the identity tokens expressed as commitments.

used to securely distribute a message to a group of Users. The Users in the group share a symmetric key(group key) with which the message is encrypted while broadcasting in the group. Since key is known to only group Users ,only they can decrypt and obtain the message. In case if group dynamics changes(any member leaves or join the group) a new group key must be generated and re distributed in a secure way to all current group users for maintaining backward and forward secrecy. In .BGKM scheme group key is given as [Group Key= private Secrets + Public Info]

Private secrets are available only with group members and public info are commonly available to all.

E. Major Benifits

1) It offers two layer encryption techniques and has six phases as identity token issuance, policy decomposition, identity token registration, data encryption and upload, data downloading an encryption ,encryption evolution management.
2) Attribute based keys, Access control policies decomposition are the strong points of this model.
3) It ensures backward secrecy as well as forward secrecy in the event of group dynamics changes.
4) With the application of BGKM no need to setup private communication channels with all the users of the group.
5) The CDS provides a mechanism to restrict the access to subdocuments only to authorized users without learning their identity attributes.

F. Limitations

1) No implementation of querying facility.
2) At the time of two layer encryption this model faces an issue on decomposition of Access Control Policies(ACPs).
3) The re-encryption of data gives computational overhead and the distribution of keys gives communication overhead.
4) In fine grained access control –push base model ,it is difficult to maintain key secrecy in a dynamic data sharing system.

G. Comparison Table

Element/Scheme	Encryption proxy based	Clod Mask based
Architecture Inclined to	Software as a Service	Storage as a Service
Access restriction	Fine Grined Access Control/ Machine Readble Rights Expression	Fine Grained(course grained) Access Control/Attribute based access Control
Protocol	-------	Oblivious Commitment Based Envelope/Broadcast Group Key Management
Encryption	XML Encryption	Two Layer Encryption/Re-encryption
Key Management	No key Management	Group Key
Access Control Policy	XACML policy	BGKM
Proxy	Encryption Proxy	No
Signature	XML Signature	No
Hardware Authentication	Trusted Platform Module	No

Using the above comparison table we attempted to depict distinction and similarities(if any) between these two privacy preservation models.

III. DISCUSSION

Researchers attempted to present privacy preservation schemes for securing cloud data. For Access restriction they use Fine grained, Course grained, Attribute based access control. The sole idea of preserving privacy of cloud data encompasses these two factors: 1) How to restrict unauthorised access to data as well as how to limit access of a registered user in order to save complete download of productive database so that he cannot access more than his right. 2) How to restrict local administrator or cloud administrator or any other actor which deals with outsource data ,to learn about data even when they perform some intended operation .

The first one be addressed by the use of access control polices like XACML, Group key Management policy, Anonymous ID management, Two factor authentication, Threshold based scheme. And the second one be addressed by the use of Cryptographic techniques like XML Encryption, Two Layer Encryption, Proxy Encryption, Homomorphic Encryption etc.

In this paper we focus on Privacy Preserving Schemes based on encryption proxy and cloud mask(which were proposed by Ulrich Greveler et. al and Nabeel et. al) .While performing comparative study on these two privacy models we noticed that cloud mask meets following security and privacy requirements.

The Document Manager and Cloud Data Service do not learn the identity attribute of Users.

The Cloud Data Service does not learn the content of the subdocuments.

The CDS provides a mechanism to restrict the access to subdocuments only to authorized users without learning their identity attributes.

Encryption proxy based model uses hardware authentication using TPM and also it performs load balancing tasks as the clients are not bound to a single encryption proxy .Here a metadata table is used where meta information of each user's transaction are stored .The encryption proxy is the key part of the system. The decryption is only on demand and reduce time consumption while the system is booting up. With the use of XACML in rule engine the system have complex access rights together with XML signature.

In cloud mask on the event of group dynamics change entire file requires to re-encrypt this gives additional computational burden and in proxy based model encryption proxy control access given to the users and in case if proxy fails the entire system could be compromised.

IV. CONCLUSION

Cloud Computing gains popularity day by day and the data generated on internet is multiplying at a very high pace but this rapid growth of data may leads severe security and privacy concern specially data which is outsourced(whether on rest or transmit)needs

protection, In this regard various researchers proposed different schemes and models based on Cryptographic mechanism, Proxy based service models,

The encryption proxy based model uses hardware authentication using TPM and encryption is only on demand also they use XACML for controlling access of users and the entire control is on Encryption Proxy and if at any time it gets fail the entire system failure may happen.

The Cloud Mask is based on two layer encryption and uses Oblivious Commitment Based Envelope(OCBE) and Broadcast Group Key Management (BGKM) for secretly deliver messages and offers better key management. However on the event of group dynamic change re-encryption applied which leads in computational over head.

In this paper we focuses only on these twoh schemes and successfully present a comparative study on to it and rest schemes might be analysed in future discussions.

REFERENCES

[1] Jayashree Agarkhed; Ashalatha R , "A privacy preservation scheme in cloud environment"Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB),2017.
[2] M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham,"Towards Privacy Preserving Access Control in theCloud," Proc. Seventh Int'l Conf. Collaborative Computing:Networking, Applications and Worksharing (CollaborateCom '11), pp.172-180, 2011.
[3] J. K. Liu, M. H. Au, X. Huang, R. Lu, J. Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services,", Transactions on Information Forensics and Security, Vol. 11, No. 3, pp.484-497, March, 2016.
[4] HP. Pooja and N. Nagarathna, Privacy Preserving Issues and theirSolutions in Cloud Computing: A Survey, IJCSIT, Vol. 6, No. 2, pp-1588-1592, 2015.
[5] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy BasedContent Sharing in Public Clouds," IEEE Trans. Knowledge and DataEng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.
[6] J. Li and N. Li. OACerts: Oblivious attribute certificates. IEEETransactions on Dependable and Secure Computing, 3(4):340-352,2006.
[7] M. Strasser and H. Stamer, "A software-based trusted platform module emulator," in Trusted Computing – Challenges and Applications. Springer Berlin / Heidelberg, 2008, pp.33–47.
[8] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." International Journal of Distributed Sensor Networks (2014).
[9] Umar Khalid Farooqui,Ashish. K.Trevedi et al , "Architecting Distributed Domain Reducer in Cloud Environment".IJCA 40(12):24-29,2012.
[10] Jayashree Agarkhed; Ashalatha R , "A privacy preservation scheme in cloud environment"Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB),2017.
[11] U. Greveler, B. Justus, D. Loehr, A Privacy Preserving System for Cloud Computing, ICCIT, IEEE, pp- 648 - 653, 2011.
[12] Mark D. Ryan, "Cloud Computing Privacy Concerns on Our Doorstep," Communications of the ACM 54(1): 36-38, 2011.
[13] M.Thangavel,S.Sridhar, "An Analysis of privacy preservation schemes in cloud computing",2nd IEEE International Conferenceon Engineering & Technology ,March 2016.
[14] Umar Khalid Farooqui,P.K.Bharti ,et . al. "A Review: privacy preservation in Cloud Environment issues and challenges",IJRASET Volume 5 Issue VIII , 2017.