IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

A Comparision of Access Control Schemes for Cloud Data Privacy

Umar Khalid Farooqui[1*], Ajay Kumar Bharti[2]

[1,2]Dept. of Computer Science & Engineering, MUIT, lucknow,Uttar Pradesh, India

[*]*Corresponding Author: uk.farooqui @gmail.com*

Available online at: www.ijcseonline.org

Accepted: 15/Oct/2018, Published: 31/Oct/2018

***Abstract*—** Cloud deliver awesome comfort to its users as the user experience cloud services without having own hardware infrastructure. Now a day's cloud services have important role on the internet as most of the services used by us are either cloud based or likely to be migrated in to cloud. The open architecture of cloud invites various security and vulnerability issues. The user data are outsourced and there is no strong privacy present between the user and cloud server because cloud uses third party intervention (which generally access the user data and auditing them). Outsourcing cloud data leads various vulnerability and privacy issues. Many researchers proposed different technique to address privacy preservation in the cloud computing, but still they are not 100% succeeded, some of them works on fine grained access control and some advocated attribute base access control scheme. In this paper, we made an attempt to compare two renowned privacy preservation schemes based on Fine Grained and Attribute based access control mechanism

***Keywords*—**Cloud Computing,privacy preservation,Fine Grained.

I. INTRODUCTION

CLOUD COMPUTING is a computing where the computer machine is virtually hosted on internet that permits establishments to shop for, rent, sell, or provide software and different digital assets through the internet whenever requested for services. CLOUD computing is an optimistic facts era structure for organizations and people. Cloud Computing facilitates the most advance data storage(SSD) and communicative paradigm with apparent pros, which include on- demand self-services, ubiquitous community get entry to, and area unbiased useful resource pooling [9]. "Cloud computing is a resources provisioning system which delivers its service on demand over Internet" [7]. "The amount of data produces and managed by cloud is highly appreciated day by day with the advent of next generation technologies" [1]. 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 give the security for outsourced data and promise the flexible and reliable services to the client. They 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 [1].

Rest of the paper is organized as follows, Section I contains the introduction of privacy preservation schemes, Section II contain the related work of privacy preservation techniques, Section III contain Analysis of privacy preservation schemes Section IV contain the discussion, section V concludes research work with future directions.

II. RELATED WORK

An Unidentified ID based data sharing algorithm abbreviated as (AIDA) which was proposed as multi-party system for cloud and distributed environment (By Dunning and Kresman) Unidentified ID based facts sharing uses set of rules for the cloud system in distributed and multi-party environment. It offers an integer records sharing set of rules and gives a unlimited anonymous assignments. Theorems of newton and sturm are used for data mining[8].Some other useful contribution in this regard are outlined below

- Attribute-Based Cryptosystem[15]
- Access Control with Security Device
  Security Mediated Cryptosystem[16]
  - Key-Insulated Cryptosystem
- BBS+ Signatures

- BBS+ is signature scheme
- CL-signature is the another name of BBS+ signature [12]
- Refer as credential signature [7]
- Useful in certifying
- Used to certify a fixed of credentials [2]

III. ANALYSIS OF PRIVACY PRESERVATION SCHEMES

Hong Liu

H. Liu et al. analyzes as " prevailing solutions recognition on the illegal get access of data, not on privatives problems when facts sharing to others" [5]. "Shared Authority based totally Privacy preserving Authentication protocol" (SAPA) proposed by Hong Liu. SAPA protocol attains the shared entry level authority by mechanisms of identifying anonymous entry with the concern of privacy and security .

© 2018, IJCSE All Rights Reserved

Access control of an attribute based is used to ensure that the particular client has the right to get his own data field only. Re-encryption of proxy is carried out to show information sharing between multiple users [4].

SYSTEM MODEL

Following figure 1 shows system model used in cloud database(storage)architecture [6].The model uses three actors playing role in the proposed system,these are client,server and third party. Below table summarizes notations used by H.Liu.

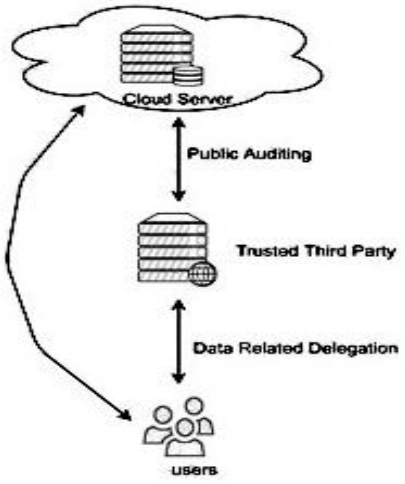

Fig 1: The Cloud Storage System Model

Client:- An individual or organization entity, who owns its statistics stored inside the cloud for web statistics persistence and computing. Versatile clients may be affiliated with the same org., and are assigned with independent set of rule on specific data fields.[6]

Table 1: Notations

Notation	Description
S, U_x	The cloud server, and a user (i.e., cloud data owner).
PID_{U_x}	U_x's pseudorandom identifier (pseudonym).
T_{U_x}	U_x's identity token that is assigned by S.
sid_{S_x}, sid_{U_x}	The pseudorandom session identifier of S, U_x.
α, σ, β, r_{U_x}	The randomly generated numbers.
$R_{U_x}^{U_y}$	The access request pointer that represents U_x's access desire on U_y's data fields.
D_{U_x}, $\dot{D}_{U_x}$	U_x's own authorized data fields, and U_x's temp authorized data fields.
A_{U_x}, L_{U_x}, P_{U_x}	The data attribute access list, re-structure data access list, and data access policy.
$\{mpk/msk\}$	The pairwise master public/privacy keys.
$\{pk/sk\}$	The pairwise public/privacy keys.
k_{Σ_x}, k_{U_x}	The aggregated keys, and the re-encryption keys.
V^{ℓ}	The locally computed value V according to the same algorithm.
C_{S_x}, C_{U_x}	The ciphertexts.
$\mathcal{F}_{S_x}(x, P_{U_x})$	The defined polynomial owned by S.
$\mathcal{F}_{U_x}(x, L_{U_x})$	The defined polynomial owned by U_x.

Server :- An entity, which is controlled by using a specific cloud provider or cloud app operator to facilitate information persistence and computing services. The server in the cloud is an entity with unlimited persistence capability and computational sources.[6]

Third Party:- Some selective and neutral entity who looks for the advanced aspect on behalf of the clients, to carry out records public-auditing and dispute-arbitration.[6]

The system model, suppose the communication channel from one to another point among the different clients and cloud server are secure by the "secure shell protocol". The authentication handshakes are not listed within these protocol presentations. There are not fully trustable relationships among a server of cloud(S) and the cloud client or user Ux [6].

SHARED AUTH. BASED PPAP

- *System Initialization:-*
  - CLOUD SERVER (S)
  - USERS (Ux)

Thereinto, Ua and Ub are 2 user, that have unrestricted access auth.on their own data field[8].

- The Proposed Protocol Descriptions: -

Relation among Ua, Ub, S, in which both Ua and Ub have the right of authorized information set for facts(data) sharing. Remember that concurrent interactions might not be synchronously launched, and certain time gap(interval) is allowable [6].

ANALYSIS OF FORMAL SECURITY BY THE UCM (UNIVERSAL COMPOSABILITY MODEL)

The UCM specifies a method for protection proofs [13], There is a real-global simulation, a really ideal-international simulation, and Sim (type of simulator) converting the protocol exe. from the real-world to the correct-global. [6]

Theorem 1. UC Security.

- Z distinguishes among relation of A with Pi,
- relation of A~ with P~i, is at most negligible possibility,
- real protocol p UC-realizes an ideal functionality F,

The UC formalization of the SAPA incorporates the idealworld model Ideal, and real-global model real

Ideal: - Declare 2 uncorrupt idea func.

1. Faccess
2. Fshare [6].

A dummy part P~ and an ideal adversary A~. {P~, A~} cannot establish direct communications.

Real: - define Pshare (run by P, Uu and S) along with Real adversary(A) and environment (Z)

© 2018, IJCSE All Rights Reserved

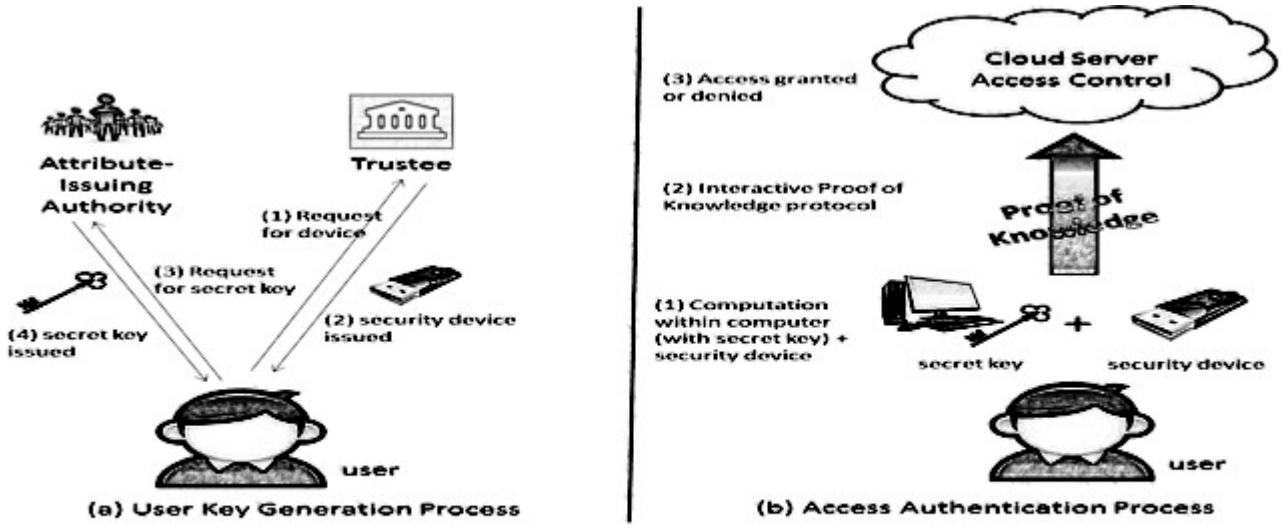

Fig 2: Overview of Fine Grained Two-Factor Access Control for Cloud Computing Services

Joseph K. Liu

For computing services based on web, J. K Liu et al. designed a "Fine Grained 2 Factor Authentication access control system" [2]. With the help of secret key and a device, they designed attribute based access control scheme. They design the system in different way ,and do not part the secret key. Instead, they proposed some additional peculiar facts preserved with the security-device. During authentication it is require that this piece of fact come together with the user secret key. In any case missing either part result in non authentication. The methodology used is pictorially represented in the above diagram.

The system comprises of under mentioned participants

• Trustee: Which is initiating all system variables and also initiate the security device.

• Attribute-issuing Authority: Which is responsible to initiate secret key for users based on their attributes.

• Users: Which is the actor who did authentication with the server. Each user bears a secret key issued by the issuing authority also a security equipment is initialized by the trustee.

• Cloud Service Provider:Which offers services to anonymously authorized clients. During authentication process it communicates with the user. Fig 2 depicts overview of 2F Access Control system.

Assumptions : Their aim was to preventing private information exposure in the event of authenticating access. Thus they come up with some hypothesis on system setup and communication channel while assuming each user communicates with the service provider through an anonymous means [17], [18] or uses IP-hiding technology. They also assume that trustee initiates the security criterion according to the algorithm prescribed. Other vulnerabilities and risks , like IP hijacking, distributed denial-of-service attack, man-in-the-middle attack, etc., were not considered by them.

Table 2: COMPARISION TABLE

ASPECTS/PAPER	***H. Liu***	***J.K. Liu***
ACCESS CONTROL	Control Access fully **Attribute** based	**Fine Grained** Access Control
KEY MANAGEMENT	Key Management is done by **Broadcast Group**	Secret key, public key, and signing algo.
POLICY	NO Policy Present here	**Two factor authentication**
ENCRIPTION	Uses **Proxy re-encryption**	Yes (SEM model for cryptography)
SIGNATURE	Not Available	BBS signature (Boneh-Boyen-Shacham)
CENTRAL AUTHORITY	No	NO

© 2018, IJCSE All Rights Reserved

IV. DISCUSSION

In the context of comparison, both researcher have proposed different techniques and methods to ensure the privacy preservation scheme. researchers are giving the access control through attribute based and fine grained based mechanism and also use of encryption for securing the cloud data. Table 2 depicts a comparative picture of both work.

Anonymous ID based data sharing is not flexible because of more complexity and if at any time the proxy compromised in the proxy based access, the entire system becomes failure.
Many cryptography techniques are defined but all the technique not confirming the privacy of the cloud data.

In the next approach the use of secret key along with the facts stored in device used for authentication is not the best solution for accessing the data because if we lost any one of them it may lead great trouble for us.

V. CONCLUSION

Now a day approximately every company upload their data on cloud because cloud computing gives many facilities to its user but the main problem is the privacy and security aspects. Author H-Liu have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity.

Whereas author J.k.Liu have presented a new 2FA including
both user secret key and a lightweight security device, Which was attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy.
Researchers proposed privacy solutions which appears working well but not found as optimal privacy solutions so, the cloud needs to give more secure services by using advance cryptography technique and advance proxy mechanism.

REFERENCES

[1] M.Thangavel,S.Sridhar, "An Analysis of privacy preservation schemes in cloud computing",2nd IEEE International Conferenceon Engineering & Technology ,March 2016.

[2] 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.

[3] Umar Khalid Farooqui,P.K.Bharti ,et . al. "A Review: privacy preservation in Cloud Environment issues and challenges",IJRASET Volume 5 Issue VIII ,2017

[4] M. Thangavel, P. Varalakshmi, S. Sridhar, "An Analysis of Privacy Preservation Schemes in Cloud Computing", 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

[5] H. Liu, H. Ning, Q. Xiong, L.T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, pp241-251, January, 2015.

[6] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.

[7] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." International Journal of Distributed Sensor Networks (2014).

[8] L.A. Dunning, R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", Transaction on Information Forensics and Security, IEEE, Vol. 8, No. 2, pp. 402-413, February, 2013.

[9] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.

[10] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in Proc. 5th Int. Conf. SCN, 2006, pp. 111–125.

[11] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in Advances in Cryptology. Berlin,Germany: Springer-Verlag, 2004, pp. 56–72.

[12] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN), Amalfi,Italy, Sep. 2002, pp. 268–289.

[13] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Proc. 42nd IEEE Symp. Foundations of Computer Science (FOCS '01), pp. 136-145, Oct. 2001.

[14] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures,"in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.

[15] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Topics in Cryptology, vol. 6558. Berlin, Germany: Springer-Verlag, 2011, pp. 376–392.

[16] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82,

[17] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in Proc. WPES, 2005, pp. 61–70. 2004.

[18] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," in Proc. 5th Int. Workshop Secur. Protocols, 1997, pp. 25–35

Authors Profile

Mr. Umar Khalid Farooqui pursed Bachelor of Science from KNIPSS, UP in 1998 and Master of Computer Application from Agra University in year 2002. He is currently pursuing Ph.D.from MUIT,Lucknow since 2015. He has published more than 10 research papers in reputed international journals and National/International conferences and it's also available online. His main research work focuses on Privacy preservation schemes and techniques, Cloud Security and Privacy, Cloud Architecture,. He has 15 years of teaching experience and 4 years of Research Experience.

Mr Ajay kumar Bharti is professor and dean in the faculty of computer science,MUIT,Lucknow ,u.p,India.His research interest is in SOA,ICT and E-Governance,cloud computing.He has published numberof research papers in International journal and confrences. He has also reviewed various reputed journals.He has more than 15 years of teaching and 6+ years of research experience.

© 2018, IJCSE All Rights Reserved