Access Control and User Authentication Concerns in Cloud Computing Environments

[1]Mohammad Ahmadi
Faculty of Computing
Asia Pacific University of Technology and Innovation
Kuala Lumpur, Malaysia
ahmadi@apu.edu.my

[2]Milad Chizari
Dept. of Electrical Engineering
Yadegar -e- Imam Khomeini (RAH) Branch,
Islamic Azad University, Tehran, Iran
milad.chizari@yahoo.com

[3]Mohammad Eslami
Dept. of Electrical & Computer,
College of Engineering, Islamic
Azad University, Zahedan, Iran
mohammad.eslami@chmail.ir

[4]Mohammad Javad Golkar
Faculty of Electrical and Computer
Imam Mohamad Bagher University
Sari, Iran
javad.golkar.1368@gmail.com

[5]Mostafa Vali
Faculty of Computing
Asia Pacific University
Kuala Lumpur, Malaysia
ahmadi@apu.edu.my

***Abstract*— Cloud computing is a newfound service that has a rapid growth in IT industry during recent years. Despite the several advantages of this technology there are some issues such as security and privacy that affect the reliability of cloud computing models. Access control and user authentication are the most important security issues in cloud computing. Therefore, the research has been prepared to provide the overall information about this security concerns and specific details about the identified issues in access control and user authentication researches. Therefore, cloud computing benefits and disadvantages have been explained in the first part. The second part reviewed some of access control and user authentication algorithms and identifying benefits and weaknesses of each algorithm. The main aim of this survey is considering limitations and problems of previous research in the research area to find out the most challenging issue in access control and user authentication algorithms.**

***Index Terms* — Cloud Computing, Access Control, User Authentication, Security, Privacy.**

I. Introduction

Cloud computing is a newfound technology that has undeniable growth in IT industry. This survey has been prepared according to three main purposes: The first purpose is describing an overall overview about cloud computing concepts, security issues in cloud computing, access control methods, and challenging issues in user authentication process. The second aim is reviewing some of access control and user authentication algorithms and identifying benefits and weaknesses of each algorithm. The last goal of this survey is considering limitations and problems of previous research in the research area to find out the most challenging issue in access control and user authentication algorithms.

According to these tasks, the research has been prepared and described to provide the overall information about the research area and specific details about the identified issues in access control and user authentication researches.

II. Cloud Computing and the Most Challenging Issue

Cloud computing is new model of widely distributed computing that users the concepts of virtualization and storage to store resources and share them between computers and other devices [1]. In this emerging technology, *users can deal with a service without any clue of where the actual infrastructure is located and what technology is used behind the scenes to manage and control the infrastructure* [2]. Despite to the several advantages of cloud computing such as unlimited storage and increasing the efficiency of computing processes, there are several concerns about the security and privacy in cloud computing environments. Figure 1 shows the advantages and disadvantages of cloud computing in brief [3].

Fig. 1. Pros and Cons in Cloud Computing

978-1-4799-7315-6/15/$31.00 ©2015 IEEE

One of the most challenging issues in cloud computing environments is managing access controls and user authentication in public and private cloud and for sharing or individual processes [4]. According to these issues, there are many algorithms and models that were identified and described by several researchers to resolve these challenging problems. Some of these algorithms and models have been described in next section to identifying the strengths and weaknesses of each research or product.

III. Access Controls and User Authentication Models

There are several access control and user authentication models that were proposed to enhance the rate of reliability in cloud computing environments. Wan *et al.* [5] proposed a cloud computing model with five types of parties:

- Data storage service was provided by **Cloud Service Provider (CSP)** by managing cloud servers.
- Data files were encrypted by **Data Owners** and were stored in cloud servers to sharing with others.
- Encrypted data files were downloaded and decrypted by **Data Consumers** according to their interest and permissions.
- **Domain Authority** is a service to access data owners and data consumers according to administration rules.
- **Truseted Authority** manages domain authority according to the rules of parents domain authority

Figure 2 (Wan *et al.* 2012) shows these five parties in details:

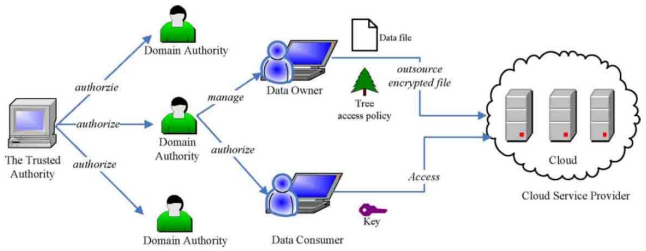

Fig. 2. Cloud Computing Five Parties (Wan *et al.* 2012)

According to this model, domain authorities are managed by trusted authority and by this management, data owner and data customers trust about the access control and their permissions. Moreover Wan's proposed model by is based on hierarchical attribute based encryption by extending the attribute policy with a hierarchical structure of users. This model provides scalability due the defined structure and fine-grained access control and flexibility in comparison with Attribute Set Based Encryption and Access Control Model (ASBE).

In 2010, Li *et al.* [6] proposed a model to achieve fine-grained access control based on attribute encryption by preventing the illegal key sharing among colluding users is missing from the existing access control systems based on attribute based encryption. For this purpose, access control policies based on data attributes was defined and enforced. Moreover, in this model, user accountability was implemented by using traitor tracing and broadcast encryption methods to support user grant and revocation. The following figure shows the architecture of the suggested model by Li *et al.* (2010): in this model, user accountability was implemented by using traitor tracing and broadcast encryption methods to support user grant and revocation. Figure 3 shows the architecture of the suggested model by Li *et al.* (2010):

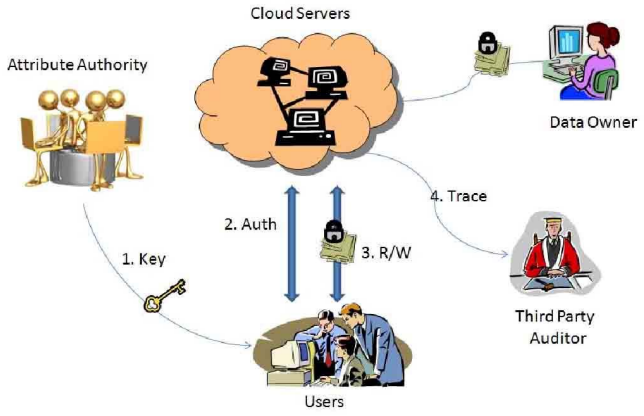

Fig. 3. Architecture of Li's Model (Li *et al.* 2010)

According to this figure, the proposed model analysis shows that this confidentiality and fine-grained access control is efficient and practical in real cloud computing environments but in this model the granularity is limited by the size of the attribute set that is associated with the encryption. This is the most challenging weakness of this model.

Wang et al. [7] suggested an adaptive access control model by trust introduction in cloud computing environments by using role based access control methods to resource management and access control decision during the communication processes in cloud computing environments.

Moreover in the proposed model, a dynamic and trust based access model was suggested to determine the security level and access control based on dynamic user authentication and controlling the user's malicious behaviour effectively. Figure 4 shows the Wang's (2011) dynamic and trust based in brief:

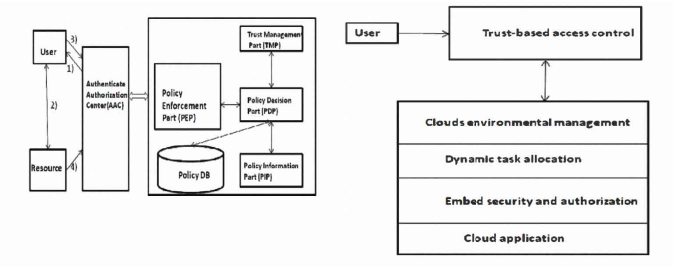

Fig. 4. Wang's Access Control Model (Wang *et al.* 2011)

According to this figure, a dynamic and trust based access model was suggested to determine the security level and access control based on dynamic user authentication and controlling the user's malicious behaviour effectively. The most important advantage of this model is extending the trusted computing technology to the communications in cloud computing environments to increase the reliability of this newfound technology.

Because of the weaknesses of Wang's model, a trust-based dynamic access control model for cloud computing environment was presented by Tan *et al.* [8] for legal identities validation and privileges access control acquiring for resources by users according to role based and trust based techniques. The authorization flow of this trust-based dynamic access control model has been shown in figure 5 (Tan *et al.* 2010):

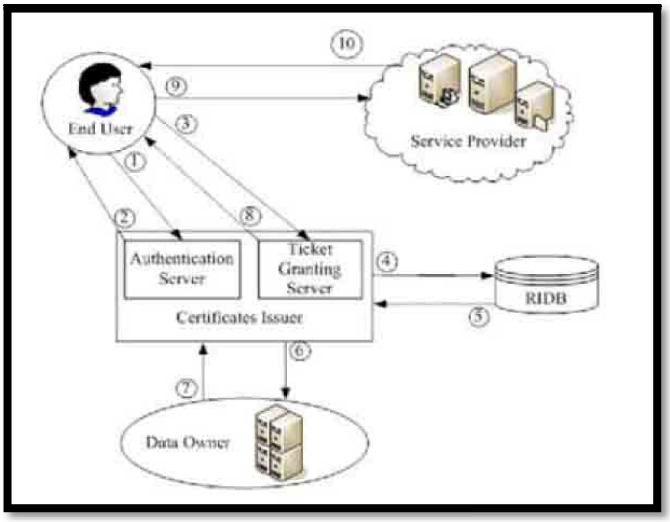

Fig. 5. The authorization flow of access control model (Tan *et al.* 2010)

According to Figure 5, the theoretical analysis of the Tan's model showed that the proposed model might be effective for providing a dynamic a secure access control.

Yu *et al.* [9] described a scheme based on data confidentiality, and scalability simultaneously to implement a fine grained data access control in cloud environments by exploiting key policy attribute based encryption and using proxy and lazy re-encryption techniques.

By using this model, delegation of most computation overhead to powerful cloud servers could be possible for data owner and confidentiality of user access privilege and user secret key accountability might be achieved. An exemplary case in the proposed model in a healthcare scenario has been shown in following figure (Yu *et al.* 2010):

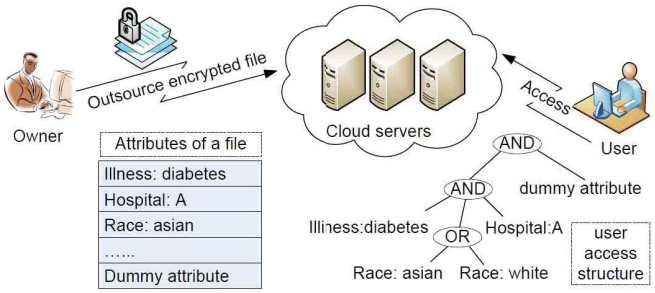

Fig. 6. An exemplary case in healthcare scenario (Yu *et al.* 2010)

For achieving to the purposes of this model, each data file the owner assigns a set of meaningful attributes, which are necessary for access control. These attributes need a huge data header for each data packet. The following figure (2010) shows an example for data header in the proposed model:

Notation	Description
PK, MK	system public key and master key
T_i	public key component for attribute i
t_i	master key component for attribute i
SK	user secret key
sk_i	user secret key component for attribute i
E_i	ciphertext component for attribute i
I	attribute set assigned to a data file
DEK	symmetric data encryption key of a data file
P	user access structure
L_P	set of attributes attached to leaf nodes of P
Att_D	the dummy attribute
UL	the system user list
AHL_i	attribute history list for attribute i
$rk_{i \to i'}$	proxy re-encryption key for attribute i from its current version to the updated version i'
$\delta_{O,X}$	the data owner's signature on message X

Fig. 7. Yu's Model Attributes Definition (Yu *et al.* 2010)

In 2012, a matrix based access control model was presented by Ilanchezhian *et al.* [10] to improve the current security model and efficiency in cloud computing environments. *"In access matrix model, when a subject wants to access an object already the access rights to access the subject by a corresponding object will be stored."* Because of this reason, when a subject requests to access an object for reading or writing process every time, the access is not granted directly instead the table is checked first. Using data hiding,

978-1-4799-7315-6/15/$31.00 ©2015 IEEE

partial request and data grouping techniques helped the proposed algorithm to decrease the taken time for unwatched requests by eliminating several requests.

F. Fatemi Moghaddam [11] suggested a cloud-based single-sign-on algorithm as an effective solution to increase the efficiency of user authentication processes in cloud-based applications according to the limitations [12] and weaknesses of similar client-based models. The proposed model was designed and described by establishing two cloud servers for storing encrypted account details and cryptography keys. Moreover, a cloud-based SaaS application was designed to connect clients and SaaS service providers. Using AES-256 and SSL in the suggested model improves the security of cloud-based SSO algorithm.

In addition, Fatemi Moghaddam et al. [13] proposed an efficient and scalable user authentication scheme in 2014. In the suggested model, various tools and techniques were introduced and used by using the concept of agent. Therefore, a client-based user authentication agent was introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a-service application was used to confirm the process of authentication for un-registered devices. Moreover, there are two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In overall, the theoretical analysis of the suggested scheme showed that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments.

According to the process of reviewing performed researches and manufactured products, several models were proposed and presented to resolve the security problems such as user authentication, access control management, and personalization process in cloud computing environments. However, each model has specific strengths and also weaknesses.

IV. Conclusion

In this paper user authentication and access control concerns in cloud computing environments were considered. As was explained, security concerns are the most challenging issues in cloud computing environments as an emerging technology. Hence, access control and user authentication procedures as two of the most important parts of security issues [14] have been specified in this research. Therefore, cloud computing benefits and disadvantages were explained in the first part. The second part reviewed some of access control and user authentication algorithms and identifying benefits and weaknesses of each algorithm. The main aim of this survey is considering limitations and problems of previous research in the research area to find out the most challenging issue in access control and user authentication algorithms.

The results showed that each model has specific strengths and also weaknesses, and none of them could provide all of the users and enterprises expectations about a security model in cloud computing environments. Having said and according the security concerns that still unclear in cloud computing communications, a harder efforts seem to be necessary to find out a reliable and more efficient user authentication and access control model in cloud-based environments.

References

[1] F. Fatemi Moghaddam, O. Karimi, and M. T. Alrashdan, "A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments," in *Proc. of 2nd International Conference on Cloud Networking (CloudNet)*, San Francisco, CA, 2013, pp. 185–189.

[2] Baker, M. Mackay, and M. Randles, "Eternal Cloud Computation Application Development." *Developments in E-systems Engineering (DeSE)*, pp. 392-397, 2011.

[3] Dion Hinchcliffe, "Eight ways that cloud computing will change business," *ZDnet Website*, 2011, [Online] Available on: http://www.zdnet.com/blog/hinchcliffe/eight-ways-that-cloud-computing-will-change-business/488, Last Accessed: May 4th, 2014.

[4] F. Fatemi Moghaddam, N. Khanezaei, S. Manavi, M. Eslami, and A. Samar, "UAA: User Authentication Agent for Managing User Identities in Cloud Computing Environments," in *IEEE 5th Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, 2014, pp. 208–212.

[5] Z. Wan, J. Liu, and R.H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" *IEEE Transactions on Information Forensics and Security*, vol.7, no.2, pp. 743-754, 2012.

[6] J. Li, G. Zhao, X. Chen, D. Xie, C. Rong. W, Li, L, Tang, and Y. Tang, "Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing," in *Proc. of IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 2010, pp. 89-96.

[7] W. Wang, J. Han, M. Song, and X. Wang "The Design of a Trust and Role Based Access Control Model in Cloud Computing," in *Proc. of 6th International Conference on Pervasive Computing and Applications (ICPCA),* 2011, pp. 330-334.

[8] Z. Tan, Z. Tang, R. Li, A. Sallam, and L. Yang "Research on trust-based access control model in cloud computing,"in *Proc. of 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 2011, vol.2, pp. 339-344.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in *Proc. of IEEE INFOCOM, 2010*, pp. 1-9.

[10] J. Ilanchezhian, V. Varadharassu, A. Ranjeeth, and K. Arun, "To improve the current security model and efficiency in cloud computing using access control matrix," in *Proc. of Third International Conference on Computing Communications & Networking Technologies (ICCCNT)*, 2012, pp. 1-5.

978-1-4799-7315-6/15/$31.00 ©2015 IEEE

[11] F. Fatemi Moghaddam, O. Karimi, and M. Hajivali, "Applying a Single Sign-On Algorithm based on Cloud Computing Concepts for SaaS Applications," in *IEEE Malaysia International Conference on Communications (MICC)*, 2013, pp. 335–339.

[12] J. Ju, Y. Wang, J. Fu, J. Wu, and Z. Lin, "Research on Key Technology in SaaS," in Proc. International Conf. on Intelligent Computing and Cognitive Informatics (ICICCI), Kuala Lumpur, 2010, pp. 384-387.

[13] F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. Kohpayeh Araghi, N. Morad Alibeigi, and S. Dabbaghi Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments," in *IEEE Region 10 Symposium*, 2014, pp. 508–513.

[14] F. Fatemi Moghaddam, R. Roshan Ravan, T. Khodadadi, Y. Javadianasl, and A. Halalzadeh, "SUAS: Scalable User Authentication Scheme for Secure Accessing to Cloud-Based Environments," in *IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2014, pp. 33–38.

978-1-4799-7315-6/15/$31.00 ©2015 IEEE