International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Authentication and Access Control for Cloud Computing Comparing Problem Issues and Solutions

Prof. Rohini S. Pawar[1], Prof. Sairabi H. Mujawar[2]

[1]*Ph.D. Research Scholar, Department of Computer Technology, BVJNIOT, Pune, India.*
[2]*Ph.D. Research Scholar, Department of Computer Technology, BVJNIOT, Pune, India.*

Abstract – *Now a day's all users to used latest technology and currently most popular cloud based system or technique. But in this technique is very useful and fast. What about the security and its major problems. In this paper we discusses about pros and cons. The emergence of pervasive cloud computing has supported the transition of physical data and machine into virtualization environment. However, security threat and privacy have been identified as a challenge to support the widespread adoption of cloud among user. Moreover, user awareness on the importance of cloud computing has increase the needs to safeguard the cloud by implementing access control that works on dynamic environment. Therefore, the emergence of Risk-Adaptable Access Control (RAdAC) as a flexible medium in handling exceptional access request is a great countermeasure to deal with security and privacy challenges. However, the rising problem in safeguarding users' privacy in RAdAC model has not been discussed in depth by other researcher. This paper explores the architecture of cloud computing and defines the existing solutions influencing the adoption of cloud among user. At the same time, the obscurity factor in protecting privacy of user is found within RAdAC framework. Similarly, the two-tier authentication scheme in RAdAC has been proposed in responding to security and privacy challenges as shown through informal security analysis.*

Key words: *Security; privacy, Access Controls, cloud computing; risk access control; authentication.*

1. INTRODUCTION

There has been a growing trend to store data in the cloud with the dramatic increase in the amount of digital information such as consumer's personal data to larger enterprises. They want to back up databases or store archival data. Cloud data storage can be attractive for users (individuals or enterprises) because it provides unpredictable storage demands, requiring cheap storage tier or a low cost and long-term archive. Service providers can focus more on the design of functions for enhance user experience of their services without worrying about resources to store the growing amount of data by outsourcing clients data to the cloud. Cloud can provide on demand resources so it can help service providers to decrease their maintenance costs. Besides, cloud storage can give a flexible and convenient way for users to access their data from anywhere on any device or gadget. There are distinctive sorts of infrastructures associated with a cloud. A public cloud is a cloud which is made accessible to the general public and also resources are allocated in a pay-as-you-go manner. A private cloud is an internal cloud that is built and operated by a single organization or association. The organization has full control on the private cloud. The private cloud cannot be accessed by external parties. Thus a private cloud is frequently considered to be more secure and trusted.

1.1 Related Work

Now a day, secure data access control has become one of the major concerns in a cloud storage system. As a logical combination of attribute-based encryption and attribute-based signature, attribute-based signcryption (ABSC) can provide con_dentiality and an anonymous authentication for sensitive data and is more ef_cient than traditional ``encrypt-then-sign'' or ``sign-then-encrypt'' strategies. Thus, ABSC is Suitable for _ne-grained access control in a semi-trusted cloud environment and is gaining more and more attention in recent years.

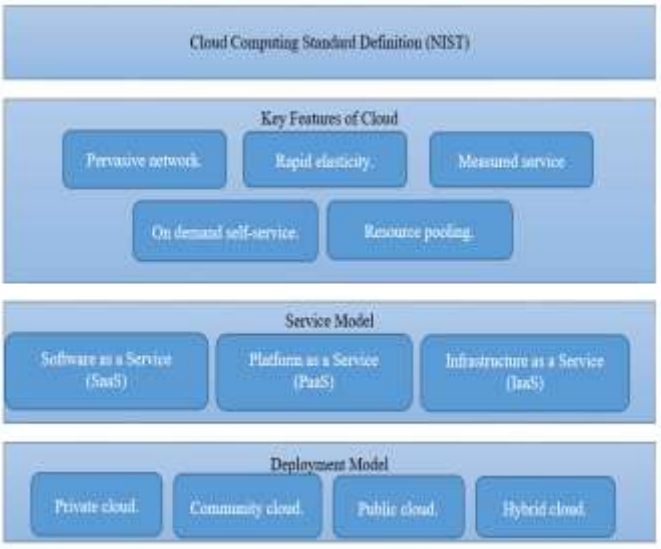
1.2 Problems and Solutions.

Table- 1: SECURITY ISSUE AND EXISTING SOLUTION IN CLOUD COMPUTING

Author	Security Issues	Existing Solution
Subashini and Kavitha	Security, integrity, confidentiality and data access. Vulnerability in virtualization. Availability, authentication and identity management.	Intensify the Service Level Agreement (SLA). Develop security framework. Apply encryption and access control.
Zissis and Lekkas	Confidentiality and privacy. Integrity. Availability.	Effective security management. Develop security framework. Apply cryptography encryption. Implement access control.

Shahzad	□ Denial of Service (DoS). □ Cloud storage security. □ Integrity,confidentiality and data availability.	□ Secured access control. □ Effective identity management. □ Encryption during authentication.
Y. Liu et al.	□ Data and security control. □ Storage virtualization. □ Authentication.	□ Apply encryption. □ Strengthen access control. □ Effective security management.
Suzic et al.	□ Identity management. □ Authentication and trust.	□ Implement access control. □ Apply cryptography for encryption.
Hepsiba and J.G.R. Sathiasee-lan	□ Malicious attack. □ Denial of Service (DoS). □ Security, integrity, confidentiality and data availability.	□ Strong encryption and access control. □ Management of information security. □ Authentication protocol.

In addition, the level of privacy in the cloud environment could help to preserve the confidentiality of the data while protecting user identity. Whereas, level of reliability relies on effective cloud management by providing storage and communications to cater user needs. Thus, the level of privacy and reliability are the dependent factor to support the development of cloud technology in an organization.



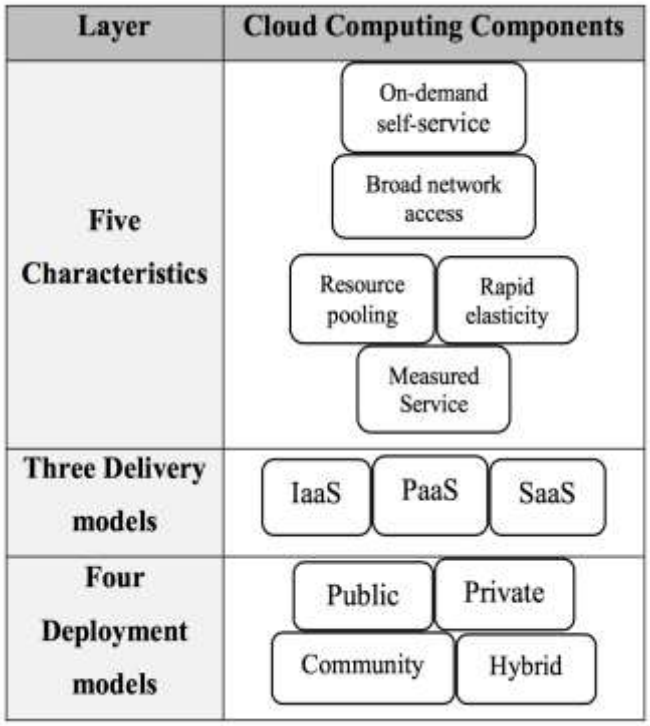


Fig- 1: Adaptation of Cloud Computing Architecture

Cloud computing is the internet-based technology that includes a storage service and communication, efficient resource management and incurs minimal cost. In addition, cloud computing imposed on virtualization technology in providing computing resources based on user's requirement [19]. Based on standard definition by National Institute of Standards and Technology (NIST), cloud computing is a model that allows network access to resources on configured computing (network, servers, applications, storage hub and services) with minimal administration or interaction [20].

Cloud computing architecture as Fig. 1 consists of four different layers which are standard definition, key features, and service and deployment model. The standard definition of cloud acts as the first layer that shape the key features of cloud computing. Next, the second layer consists of five key characteristics of the cloud that drives consumer engagement in service model and deployment model.

Sometimes they know the location at a high-level abstraction, such as country, state, and data center. Storage, processing, memory, and network are the kind of resources that are assigned. Rapid elasticity is also one of the cloud computing characteristics, which means that resources are dynamically increased when needed and decreased when there is no need. Also, one of characteristics that a consumer Needs is measured service in order to know how much is Consumed. Also, it is needed by the cloud provider in order

to know how much the consumer has used in order to bill him or her.

2. Infrastructures of Cloud Security.

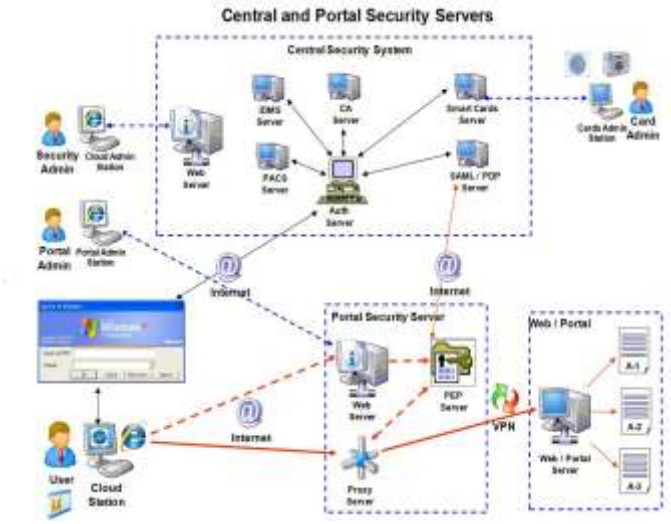


Fig- 2: Cloud Security Infrastructure1

A single enterprise may provide many application services to end-users. E-mail servers and web servers are examples of application services providers. As company's boundaries broaden, the number of application services grows. Mostly all service providers should authenticate clients before service transactions are executed, because they are dealing with personal information. This means that the client should have security context for each application server and log in before it can consume any service. The same situation happens when the client accesses resources in different security domains. As mentioned in the second chapter, having many security credentials for authentication purposes is not an effective solution from security, system coordination, and management perspectives. While organizations migrate to cloud environments, the same problem still exists.

Cloud model is composed of five essential characteristics, three service models, and four deployment models as in the figure 3. In this technology users outsource their data to a server outside their premises, which is run by a cloud provider [4]. In addition, memory, processor, bandwidth and storage are visualized and can be accessed by a client using the Internet [5]. Cloud computing is composed of many technologies such as service oriented architecture, virtualization, web 2.0 and more. There are many security issues with cloud computing. However, the cloud is needed by organizations due to the need for abundant resources to be used in high demand and the lack of enough resources to satisfy this need. Also, cloud computing offers highly efficient data retrieval and availability. Cloud providers are taking the responsibility of resource optimization.

Fig- 3: Schematic definition of cloud computing

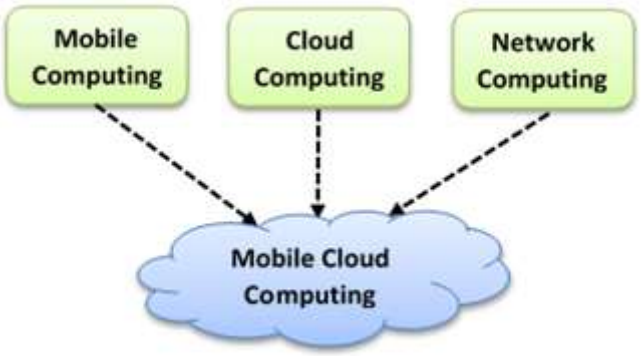
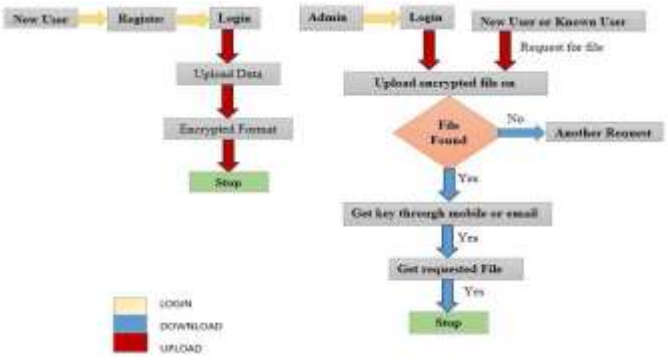


Fig- 4: Cloud Security Infrastructure2

Mobile cloud computing is using the mobile as front end and the cloud as back end for the storage and computation. In the figure, mobile cloud computing consists of mobile computing, cloud computing, and network. In, three schemes are proposed for confidentiality and integrity of mobile device's files stored in the cloud. The first scheme is encryption based Scheme (EnS). In this scheme, the mobile device encrypts the file and gets its hash code. The encryption key is a concatenation of the password entered by a user, file name changed to bits and file size to defend brute force attack on a cloud server since the length of the password is limited. Only the file name is kept in the file and everything related to the file is deleted. When downloading the file from the cloud server, only the password is needed to decrypt the file. This process will need more processing on the mobile device side.



Future Points.

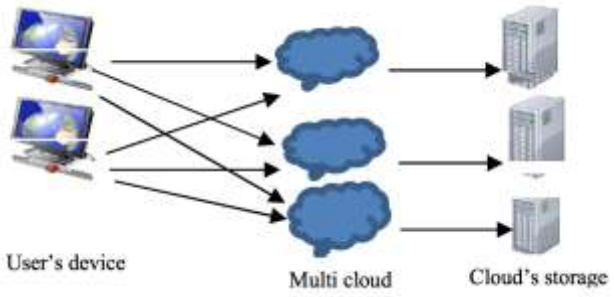


Fig- 5: Multi-cloud computing

Cloud computing now is moving to multi-cloud computing Because of security issues stemming from using a single cloud such data availability. This figure 16 shows how the clients connect to the clouds. Some of the issues that multi-cloud computing are data availability and security , Cachinet et al. said Services of single clouds are still subject to outage. There is a fear among organizations that a single cloud would not fulfill their demands such as reliability and availability. Some organizations need the availability to be high and need their data to be far from being locked in. Therefore, they need a system that is always available and not under control of a single cloud provider.

3. CONCLUSION

Implementations of cloud security solutions under the concept of Security as a Service are in their awaking phase. This research has proposed a cloud security system based on That concept and made contributions in the area of authentication and authorization services for a cloud environment. The problem has been solved and the goals have been achieved.

ACKNOWLEDGEMENT

We are honored to work with our supervisor, **Principal R. R. Utturkar,** and we would like to thank him for his support and patient guidance during our master work.

We are also thankful to the whole **Computer Department** team for a helpful collaboration.

Finally, we would like to thank our whole **family** for their encouragement and invaluable support during this work period.

REFERENCES

[1] Meva and C. K. Kumbharana, "Issues and challenges of security in cloud computing environment.," Int. J. Adv. Netw. Appl., pp. 108–111, 2015.

[2] S. Abolfazli, Z. Sanaei, A. Tabassi, S. Rosen, A. Gani, and S. U. Khan, "Cloud adoption in Malaysia: Trends, opportunities, and challenges," IEEE Cloud Comput., vol. 2, no. 1, pp. 60–68, 2015.

[3] L. Wei et al., "Security and privacy for storage and computation in cloud computing," Inf. Sci. (Ny)., vol. 258, pp. 371–386, 2014.

[4] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Secur. Priv., vol. 8, no. 6, pp. 24–31, 2010.

[5] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, "Access control as a service for the cloud," J. Internet Serv. Appl., vol. 6, no. 1, 2015.

[6] A. H. Karp, H. Haury, and M. H. Davis, "From ABAC to ZBAC : The evolution of access control models," ISSA J., no. April, pp. 22–30, 2010.

[7] M. Mulimani and R. Rachh, "Analysis of access control methods in cloud computing," no. July, 2016.

[8] V. Boyko, P. Mackenzie, and S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman," Eurocrypt, vol. 2, pp. 156–171, 2000.

[9] Y. Zhu, D. Huang, C.-J. Hu, and X. Wang, "From RBAC to ABAC: constructing flexible data access control for cloud storage services," IEEE Trans. Serv. Comput., vol. 8, no. 4, pp. 601–616, 2015.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. Comput. Commun. Secur. - CCS '06, p. 89, 2006.

[11] A. Sudarsono, M. U. Harun, and A. Rasyid, "Secure data sensor in environmental monitoring system using attribute-based encryption with revocation," vol. 7, no. 2, pp. 609–624, 2017.

[12] D. Ricardo dos Santos, R. Marinho, G. Roecker Schmitt, C. Merkle Westphall, and C. Becker Westphall, "A framework and risk assessment approaches for risk-based access control in the cloud," 2016.

[13] B. Suzic, A. Reiter, F. Reimair, D. Venturi, and B. Kubo, "Secure data sharing and processing in heterogeneous clouds," Procedia Comput. Sci., vol. 68, no. 316, pp. 116–126, 2015.

[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[15] Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," J. Comput. Sci. Eng., vol. 9, no. 3, pp. 119–133, 2015.

[16] C. L. Hepsiba and J.G.R.Sathiaseelan, "Security issues in service models of cloud computing," Int. J.

Comput. Sci. Mob. Comput., vol. 5, no. 3, pp. 610–615, 2016.

[17] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[18] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and J. L. Hoon, "A strong user authentication framework for cloud computing," in Proceedings - 2011 IEEE Asia-Pacific Services Computing Conference, APSCC 2011, 2011, pp. 110–115.

[19] C. G. Song, N. Y. Hwang, H. C. Yu, and J. B. Lim, "A dynamic resource manager with effective resource isolation based on workload types in virtualized cloud computing environments," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 7, no. 5, pp. 1771–1776, 2017.

[20] P. Mell and T. Grance, "The NIST definition of cloud computing recommendations of the National Institute of Standards and Technology," Nist Spec. Publ., vol. 145, p. 7, 2011.

[21] B. Hari Krishna, S. Kiran, G. Murali, and R. Pradeep Kumar Reddy, "Security issues in service model of cloud computing environment," in Procedia Computer Science, 2016, vol. 87, pp. 246–251. Nurul Elliza asmin and Mohammad Khatim Hasan, "Framework for the implementation of E-Government system based on cloud computing for Malaysian public sector," Ejournal.Ukm.My, vol. 7, no. 1, pp. 1–18, 2018.

[22] Sairabi Mujawar, "Prediction of Heart Disease using Modified K-means and by using Naive Bayes", in International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 10, October 2015.

[23] Sairabi Mujawar, Prakash Devale, "Heart Disease Prediction Using Modified K Means And Using Naive Baiyes", International Journal of Computer Sciences and Engineering, Volume-3, Issue-10, 2015.

BIOGRAPHIES

Ph.D. Research Scholar, *Department of Computer* Technology, BVJNIOT, Pune, India.

Ph.D. Research Scholar, Department *of* Computer *Technology, BVJNIOT, Pune, India.* She had completed graduation in BE in Computer Engineering from Bharati Vidyapeeth college of Engineering, Mumbai University, Navi Mumbai, Maharashtra, India in 2007.