

Three Level Advanced Cloud Computing Security Mechanism

Himanshu V. Taiwade¹, Bhagyashree T. Kaley², Aditya R. Raoot³

¹Assistant Professor & H.O.D of Computer Technology ,Priyadarshini Institute of Engineering & Technology,Nagpur

²Student of Computer Technology, Priyadarshini Institute of Engineering & Technology,Nagpur

³Student of Computer Technology Priyadarshini Institute of Engineering & Technology,Nagpur

(E-mail: bhagyashreekaley@gmail.com , raootaditya@gmail.com , himanshu.taiwade@gmail.com)

Abstract— In recent years, there's boom in the cloud computing so does the cloud data hijacking & data theft risks. Security of the cloud from the client side is much more objected and is stereotyped. Most of the data is stored and retrieved from client-side and focusing to secure the cloud from the client devices.

Therefore, current limitations are discussed, on basis of those limitations another step is taken towards securing a cloud from client device, and the solution is proposed in this paper, which uses a total of 3 layer of security along with unique identity of a user as an added security layer. As well as, the future scope and advancements of the security mechanisms is suggested.

Keywords— Cloud Computing, Cloud Security, Cloud Computing Security, Cloud Security Mechanisms.

I. INTRODUCTION

Since the era of Internet begun, a small idea of cloud computing technology was taking its shape, but no one had ever thought that it will grow with such a rapid pace and will become 21st century's one of the top technologies. Now, billions of Giga bytes of data is up streamed and down streamed to and from the clouds storages. The cloud markets have reached the peaks of popularities in terms of data security and the cloud community is continuously researching & developing security mechanisms to make the cloud storages even more secured than they were yesterday [1]. Thus clients on the other side are stereotyped for lacking security and possibly suffering increased risk of cloud data hijacking & data theft. Tech Giants like Google, Microsoft & Apple had introduced their smart phones in the market, since then smart phone users are dominating the number of PC users over the network, which affected almost every website and cloud service providers to create platforms smart phone friendly, which in return had raised client side security issues eventually and quadrupled the risks of cloud computing security without a question [7]. Especially in SaaS (Software-

as-a-Service), if an employee of an organization had left the organization but still the identity of that employee can remain active for at least few days to weeks, which in return can act as a threat to confidential data getting exposed [3].

Therefore, the data breach and data stealing is a threat to consumers and the users of organizations, hence similar security issues are faced by the cloud service organizations [1]. Cloud computing Holds staggering potential to alter the way how organizations and consumers run the Information Technology and can make visible transformation in the way how hardware as well as software is being used.

II. LIMITATIONS IN CURRENT SECURITY

Doing a thorough Research on cloud security issues, it is absolutely understood that some security breaches are just cannot be avoided because of the loop-holes of the security systems. Hence there is a need of a better way out [8]. As of today, latest electronic devices & instruments such as smart glasses, smart wrist watches, wristbands, wireless infotainment system in automobiles etc. Which revolves around IOT (Internet of things) Introducing Fog & Dew computing concepts in late 2018, security demands are now sky rocketing. Many smartphones are coming with heavy duty & powerful processors than ever which can easily multitask and manage 5G internet speed. These smartphones are used to access internet thus mobile edge computing is being used [2].As explained by authors, Tian Wang, Jiyuan Zhou, Xinlei Chen, Guojun Wang, Anfeng Liu, and Yang Liu, there is an immediate need of latest data storage facilities and change the way how traditional cloud works. They had developed their algorithms and used the concept of Fog computing for data transfer and access on cloud [4].

Thus, rise of smart phones and continuously evolution of security mechanisms and features, it has been a mandatory feature given in every smart phones & laptops produced after 2014 to provide a finger print scanner or a biometric scanner [5]. And hence till year 2020-2021, even the lowest

configuration electronics (smart phones, laptops or desktops, smart wrist bands etc.) will have biometric scanners compulsory.

But effective utilization of such advanced hardware is still not yet done [6]. Society is certainly lacking to optimize the use of such robust hardware in combination with software to get results which fulfill the demands of advanced security mechanisms [9]. As of cloud security concerns and in SaaS (Software-as-a-Service), IaaS (Infrastructure as a Service) or PaaS (platform-as-a-Service), security break and data breaches are more observed in IaaS.

III. PROPOSED METHOD

As already studied about applying the randomly generated unique code verification by user [1]. In addition to that combination of additional security is proposed as shown in figure 1. Flow chart,

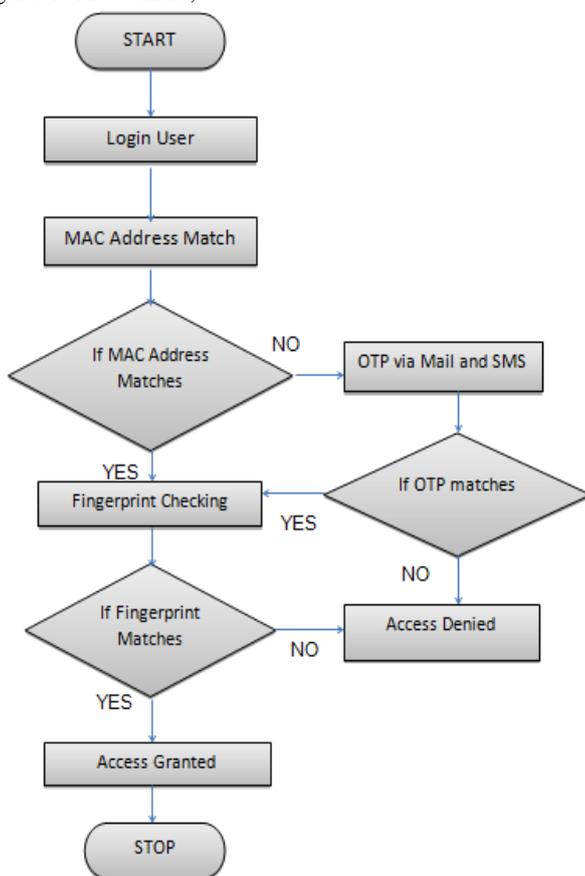


Fig.1: Representation of Data flow

Thus, 1st level of security, MAC address is first verified through the login table, If Mac address is not verified then randomly generated numeric code is send to the user's mobile

number which is registered with the user's service provider along with user registered e-mail address, 2nd level of security. In spite of the matching of Mac address, finger print verification is a compulsory step which acts as a biometric scanning & verification mechanism for cloud security, 3rd level of security. Further Mac address, OTP & Biometric scanning is successfully verified only then access is granted. If not, then access is denied in all the possible & remaining cases. Biometric scanning is an advanced security feature which can be used with other layers of security to get the combination of strongest security mechanisms which are also loop-hole free mechanisms.

IV. CONCLUSION AND FUTURE SCOPE

We can surely use various combinations of security levels in thoughtful sequence to manage the desired level of security from spectrum of low to high levels of security mechanisms depending on the requirements & cost effectiveness of the application. In future, it is possible to achieve greater and even stronger security and lower the chances of security breaches to less than today are statistics.

REFERENCES

- [1] Himanshu V. Taiwade, "Enhanced Security Mechanisms for Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015 ISSN: 2277 128X.
- [2] Yuezhi Zhou, Di Zhang, and Naixue Xiong "Post-Cloud Computing Paradigms: A Survey and Comparison", 2018
- [3] Srilakshmi Ramireddy "Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress" *AMCIS 2010*.
- [4] Tian Wang, Jiyuan Zhou, Xinlei Chen, Guojun Wang, Anfeng Liu, and Yang Liu "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing", *Member, IEEE, VOL. 2, No. 1, February 2018*.
- [5] Ekta M. Choudhari, Ketan D. Bodhe "Biometrics Authentication Technique in Cloud Computing" *IJSRE Volume 5 Issue 01 January 2017*.
- [6] S. Basu *et al*, "Cloud computing security challenges & solutions-A survey," *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2018, pp. 347-356.

[7] V. Ganapathy, S. Jajoda, C. Mazumdar, "Reflections on the Self-service Cloud Computing Project" in *Information Systems Security. ICISS 2015. Lecture Notes in Computer Science*, Springer, Cham, vol. 9478, 2015.

[8] P. Mell, "What's Special about Cloud Security?" in *IT Professional*, vol. 14, no. 4, pp. 6-8, July-Aug. 2012.

[9] X. Wang and X. Gao, "The research of a resource-aware cloud computing architecture based on web security," *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, Hangzhou, 2012, pp. 440-443