Turkish Journal of Computer and Mathematics Education Vol.11 No.03 (2020), 1402-1405
Research Article

A Survey for Comparative Analysis of various Security Methods to protect User Authentication on Cloud

Ms.Shweta Kiran Yande[a], Dr. Blessy Thankachan.[b]

[a] School of Computer and System Sciences, Research Scholar,Jaipur National university, Jaipur, Rajasthan,India. yande.shweta9786@gmail.com
[b]School of Computer and System Sciences, Associate Professor,Jaipur National university Jaipur, Rajasthan, India.

Abstract

Now-a-days there are many organization who have huge amount of data to be stored. This increases the demand for huge storage. Cloud storage is one of the solution to it. As the demand for the cloud storage is increasing, so is the security to keep data and user save is also increasing. The National Institute of Standards and Technology (NIST) defines cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient,on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned andreleased with minimal management effort or service provider interaction"[Kumar et al., 2020].Through cloud computing data can be accessed by many users simultaneously, therefore proper identification and authentication of the user is mandatory. In this survey, comparative analysis of various technique used to authenticate the user over cloud is done.

Keywords : Cloud Computing, Authentication.

1. INTRODUCTION

In today's generation the size of the data is increasing and so do the need for its storage. With the help of cloud computing problems for storing these data is solved. Cloud Computing works in a distributed manner. It not only stores the data but, make it available anytime anywhere; just need to sign in for the services.

To make avail these services of cloud, some authentication of the user is needed. Authentication is a process of identifying an individual to whom they claim[(SINGH & SINGH, 2019)]. There are traditional methods available like username and static password mechanism, where a user is asked for registration process in which he/she keeps a suitable password and then these is used for further login process. Now-a-days there are many other factor for the authentication purpose like graphical password, token based, biological based, etc. When used this password in stand-alone they are termed to be one-factor authentication process since they consider only single factor. This type of authentication is more prone to attack.

2. LITRETAURE REVIEW

In(SINGH & SINGH, 2019) , the author has made use of three level of authentication. In level 1, username and password is used with SHA-1 & AES-128 CBC. In level 2, One time password is mailed and communicated through SMS. In level 3, graphical authentication is done.

In(Tabrizchi & Kuchaki Rafsanjani, 2019), the author has focus and explores a detailed knowledge about the security challenges that are faced by cloud entities such as cloud service provider, the data owner and cloud user. A generalized view of issue has been presented to enhance the importance of understanding the security flaws of cloud computing framework & devising suitable countermeasures for them.

In(Kumar et al., 2020), the author has used two factor authentication scheme. The author is trying to secure database stored on cloud from attacker. Username and password along with OTP technique is used for user authentication.

In(ShanmugaPriya et al., 2019), the author is applying secured authentication scheme for user authentication. Generation of dynamic One Time Password for every login is done. It makes use of mobile phone for verification.

In(Jiang et al., 2018), the author describes privacy and security threats sever in VCC due to sharing of resources among unfamiliar vehicles, It describes security goals for interoperability with VCC. It provides AKA framework for VCC security (through authentication and key agreement).

In(Rizwan Ghori & Ali Ahmed, 2018), the author studied different authentication system each having its own advantages and disadvantages. Authentication system like smart card, multifactor (RSA& OTP, OTP & Challenge picture, OTP & Biometric).

In (Zhang et al., 2018), the author uses the 2-D code technology to carry out identity authentication in the cloud computing environment and QR coding technology is used as the processing technology of 2-D code. The symmetric encryption algorithm and dynamic key are used to encrypt the information of 2-D code generation.

In (Alshammari et al., 2017), the author has investigated some prime security attacks. Author has also identified some possible solution for clouds which include XML signature wrapping attacks, Browser Security and Vendor lock-in.

In (Wadhwa & Gupta, 2017), major access control models and authentication schemes proposed earlier for cloud environment are analyzed and compared over selected characteristics. A Multi-Security Level Based Authentication and Access Control Model (MLBAAC) is proposed.

In (Roy et al., 2017), the author propose a new mobile user authentication scheme for mobile cloud computing based on cryptographic hash, bitwise XOR and fuzzy extractor function. The given scheme is secure against possible well known passive and active attack and provides user anonymity. Author makes use of ProVerit 1.93 simulation, BAN (Burrows-Abadi-Needham) for proposed system.

In(Chang & Choi, 2016), the author reviews user authentication and authorization issue for secured inoperability in cloud computing. Different security issues like password guessing attack, replay attack, man-in-middle attack, masquerade attack, insider attack, phishing attack, shoulder surfing attack are studied. Algorithms with respect to encryption like RSA,AES, MD5 hashing, OTP password algorithm, DES are described.

In (Mitra et al., 2016), author suggests an efficient and simple solution for authentication in cloud computing. It investigates the nature of characteristics polynomials of Equal Length Cellular Automata (ELCA) and its application in OTP generation for authentication in cloud computing. Algorithm is designed for cost effective generation of OTPs, flexible generation of equally populated OTP sets, and generation of controllable number of password in OTP sets.

In(Namasudra & Roy, 2016), the author gives a novel authentication scheme using Chebyshev Chaotic maps. Various security factors such as scalability of login, mutual authentication, freedom of password change, 2-factorr security and forward security are proposed. The proposed model given by author is secured under the computational Diffie-Hellman assumption of Chebyshev polynomials in the random oracle model.

In(Moghaddam et al., 2014), the author has created client based user authentication agent. It is installed in end-user browser to confirm the identity of user before accessing cloud servers. Author has also made use of RSA encryption algorithm before storing data in cloud server.

In(Choksi, 2014), the author has done a survey of current cloud computing authentication trends. The author refer authentication as a mechanism that establishes the validity of the claimed identity of the individual. Four kinds of authentication methods are given as : Something an individual KNOWS, Something an individual POSSESS, Something an individual IS, Something an individual DOES. Different framework of proposed by different authors are described.

In(Ziyad & Rehman, 2014), the author has done a survey of current cloud computing authentication trends. The author refer authentication as a mechanism that establishes the validity of the claimed identity of the individual. Four kinds of authentication methods are given as : Something an individual KNOWS, Something an individual POSSESS, Something an individual IS, Something an individual DOES. Different framework of proposed by different authors are described.

In(Dinesha & Agrawal, 2012), the author has introduce multilevel authentication technique which generates password at multilevel to access cloud services. Different passwords are generated at different level of organization. First level- organization password, Second level – team level password, Third level – User level password are used.

In (Zwattendorfer & Tauber, 2012), the author try to provide authentication mechanism for sensitive aeas of cloud like e-Government. STORK framework for secure cloud authentication using eIDs is proposed.

In(Lee et al., 2010), the author has developed two factor authentication framework which implements Public Key Infrastructure (PKI) authentication and Mobile Out-Off- Band (OOB) authentication. Certificate Authority (CA) generates public key certificate and digital signature which are used for verification.

3. COMPARATIVE ANALYSIS OF SECURITY METHODS

The table 01 gives the comparison of various methods for authentication over cloud on various parameters made in the survey. The considered parameters are Complexity, Additional device, Security, etc.

Method / Parameteres	Composition	Security	Complexity	Additional Device	Cons
Numeric password	Consist of only numbers	Lowest	Simple	Not required	Easily hackable
Alphanumeric password	Consist of numbers and alphabets	Lowest	Simple	Not required	Easily hackable with different permutation and combination.
Graphical password	Makes use of some preselected pictures	Low	Simple	Not required	Requires much storage space then text based password
Static Tokens	Makes use of secret static code or number	Medium	Simple	Not required	If secret number is hacked, person identity can be misused.
Synchronous Dynamic Token	Generates random number like OTP	High	Medium	Not required	Requires time to generate OTP which may cause delay in accessing.
Challenge response Token	Uses Smartcard	High	Medium	Required	Cost for additional device
Biological features	Uses human features like fingerprint, retina	Highest	Hard	Required	Cost for additional device
Biological Characteristics	Uses characteristics like voice print.	Highest	Hard	Required	Cost for additional device

4. CONCLUSION

Cloud computing have become very popular and important to store data. The data is accessible anywhere at anytime. So it is important to authenticate the user appropriately. The authentication can be achieved with different methods available. Comparative analysis using different parameters of methods to identify pros and cons of these methods are made. This paper concludes that password based methods are easy to use, token based are complex and require more time whereas biological based requires additional devices which increase the expenses.

REFERENCES

Alshammari, A., Alhaidari, S., Alharbi, A., & Zohdy, M. (2017). Security Threats and Challenges in Cloud Computing. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 46–51. https://doi.org/10.1109/CSCloud.2017.59

Chang, H., & Choi, E. (2016). User authentication in cloud computing. *Communications in Computer and Information Science*, *151 CCIS*(PART 2), 338–342. https://doi.org/10.1007/978-3-642-20998-7_42

Choksi, S. (2014). Comparative Study on Authentication Schemes for Cloud Computing. *International Journal of Engineering Development and Research*, *2*(2), 2785–2788.

Dinesha, H. A., & Agrawal, V. K. (2012). Multi-level authentication technique for accessing cloud services. *2012 International Conference on Computing, Communication and Applications, ICCCA 2012*. https://doi.org/10.1109/ICCCA.2012.6179130

Jiang, Q., Ni, J., Ma, J., Yang, L., & Shen, X. (2018). Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing. *IEEE Network*, *32*(3), 28–35. https://doi.org/10.1109/MNET.2018.1700347

Kumar, S., Jafri, S. A. A., Nigam, N. A., Gupta, N., Gupta, G., & Singh, S. K. (2020). A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing. *IOP Conference Series: Materials Science and Engineering*, *748*(1). https://doi.org/10.1088/1757-899X/748/1/012026

Lee, S., Ong, I., Lim, H.-T., & Lee, H.-J. (2010). Two Factor Authentication for Cloud Computing. *Journal of Information and Communication Convergence Engineering*, *8*(4), 427–432. https://doi.org/10.6109/jicce.2010.8.4.427

Mitra, A., Kundu, A., Chattopadhyay, M., & Chattopadhyay, S. (2016). A cost-efficient one time password-based authentication in cloud environment using equal length cellular automata. *Journal of Industrial Information Integration*, *5*, 17–25. https://doi.org/10.1016/j.jii.2016.11.002

Moghaddam, F. F., Moghaddam, S. G., Rouzbeh, S., Araghi, S. K., Alibeigi, N. M., & Varnosfaderani, S. D. (2014). A scalable and efficient user authentication scheme for cloud computing environments. *IEEE TENSYMP 2014 - 2014 IEEE Region 10 Symposium*, 508–513. https://doi.org/10.1109/tenconspring.2014.6863086

Namasudra, S., & Roy, P. (2016). A new secure authentication scheme for cloud computing environment. *Concurrency Computation Practice and Experience*, *22*(6), 685–701. https://doi.org/10.1002/cpe

Rizwan Ghori, M., & Ali Ahmed, A. (2018). Review of Access Control Mechanisms in Cloud Computing. *Journal of Physics: Conference Series*, *1049*(1). https://doi.org/10.1088/1742-6596/1049/1/012092

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumar, N., & Vasilakos, A. V. (2017). On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. *IEEE Access*, *5*(c), 25808–25825. https://doi.org/10.1109/ACCESS.2017.2764913

ShanmugaPriya, S., Valarmathi, A., & Yuvaraj, D. (2019). The personal authentication service and security enhancement for optimal strong password. *Concurrency Computation* , *31*(14), 1–7. https://doi.org/10.1002/cpe.5009

SINGH, C., & SINGH, T. D. (2019). a 3-Level Multifactor Authentication Scheme for Cloud Computing. *International Journal of Computer Engineering & Technology*, *10*(1), 184–195. https://doi.org/10.34218/ijcet.10.1.2019.020

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2019). A survey on security challenges in cloud computing: issues, threats, and solutions. In *Journal of Supercomputing* (Vol. 76, Issue 12). Springer US. https://doi.org/10.1007/s11227-020-03213-1

Wadhwa, A., & Gupta, V. K. (2017). Proposed framework with comparative analysis of access control & authentication based security models employed over cloud. *International Journal of Applied Engineering Research*, *12*(24), 15715–15722.

Zhang, M., Ma, Z., Zhang, Y., & Wang, Y. (2018). An identity authentication scheme based on cloud computing environment. *Multimedia Tools and Applications*, *77*(4), 4283–4294. https://doi.org/10.1007/s11042-017-4552-x

Ziyad, S., & Rehman, S. (2014). Critical Review of Authentication Mechanisms in Cloud Computing. *International Journal of Computer Science Issues (…*, *11*(3), 145–149. http://www.ijcsi.org/papers/IJCSI-11-3-1-145-149.pdf

Zwattendorfer, B., & Tauber, A. (2012). Secure cloud authentication using eIDs. *Proceedings - 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, IEEE CCIS 2012*, *1*, 397–401. https://doi.org/10.1109/CCIS.2012.6664435