ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Issue 2, February 2017

Accessing Data from Cloud using Password Authentication Scheme

Pankaj Lathar[1], Dr.Yudhvir Singh[2] and Dr.Girish Kumar Sharma[3]

[1]*Research Scholar, Dept. of Computer Science & Engineering, University Institute of Engineering & Technology, M.D. University, Rohtak-124001*
[2]*Associate Professor, Dept. of Computer Science & Engineering, University Institute of Engineering & Technology, M.D. University,Rohtak-124001*

[3]*Associate Professor & Head, P.G. Dept. of Computer Science, Bhai Parmanand Institute of Business Studies,Shakarpur,Delhi-110092.(Govt. of NCT Delhi) GGSIP University*

Abstract

Cloud computing is wide technology that provides services either hardware or application services on demand. These services are used by customers to perform their tasks. The customers are getting addicted to these flexible, scalable and pay per use services provided by different cloud vendors. Keeping this in mind, the paper introduces an authentication technique by generating password at client end. It prevents third party from accessing data at client end.

Index terms

Authentication, cloud computing, cloud security and password generation

1. INTRODUCTION

Cloud computing is an amalgation of various technologies like grid computing, ubiquitous computing, services oriented architecture (SOA) and many more [1]. The technology is alluring various organizations and companies to use their application oriented services and perform tasks in lesser time. Since it utilizes services from various areas, so it must provide some security mechanisms to prevent loss of data from untrusted sites and vendors. Various cloud privacy problems are related to industry like data access, data segregation, lack of trust, lack of virtualization & verification of identity and signatures. All those issues need to be reduced so as to make secure data access from cloud. The paper devised a technique of securing data by generating OTP (One time Password) at client side.

The following paper is organized as follow: section2 presents various studies and their failures in context of cloud authentication. Section 3 describes proposed password authentication scheme. It also presents

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Issue 2, February 2017

algorithm for generating unique password at client side. Section 4 concludes the given paper.

2. LITERATURE SURVEY

Several studies have been led by researchers in context of authentication that can lead to various password generation techniques.

Zhu et.al [2] proposed graphical passwords to make secure usage of cloud services. It uses dignified image of text that is not seen by outside users. But this failed due to larger memory space than given cloud area. Waters et.al [3] also worked on showing graphical results via graphical password generator but it is very time consuming. So, it has failed. Safir et.al [4] tried to propose user identity management protocol by using text password for securing data. But it has its its limitations like text password is easy to break by brutal attacks. Goh et.al [5] proposed secure indexing model by using simple as well as graphical password technique without taking care of customer details. Kan yang et.al [6] proposed data access control mechanism for storing data in secured way. Alzain et.al [7] studied various reports in context of cloud privacy and security. Ruj et.al [8] used decentralization technique for accessing of data. But they failed to avoid risk of intruders and attackers.

3. Proposed password authentication scheme

The technique helps to secure data from untrusted sites and vendors by introducing alphanumeric and white spaces password generation technique at client end. The user is allowed to register first at cloud vendor site. Then, he/she is required to enter his personal details for completing registration process. Then, it is redirected to vender site (server side) and it generates an OTP on users personalized devices like laptops, mobiles etc. After entering OTP, users can get his login credential form that contains users name & password field. In this form, user is asked to enter username and password with alphanumeric and special characters.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Issue 2, February 2017

With this multi password generation, only particular user can access data and use services on its cloud. The layout of proposed scheme is given below:-

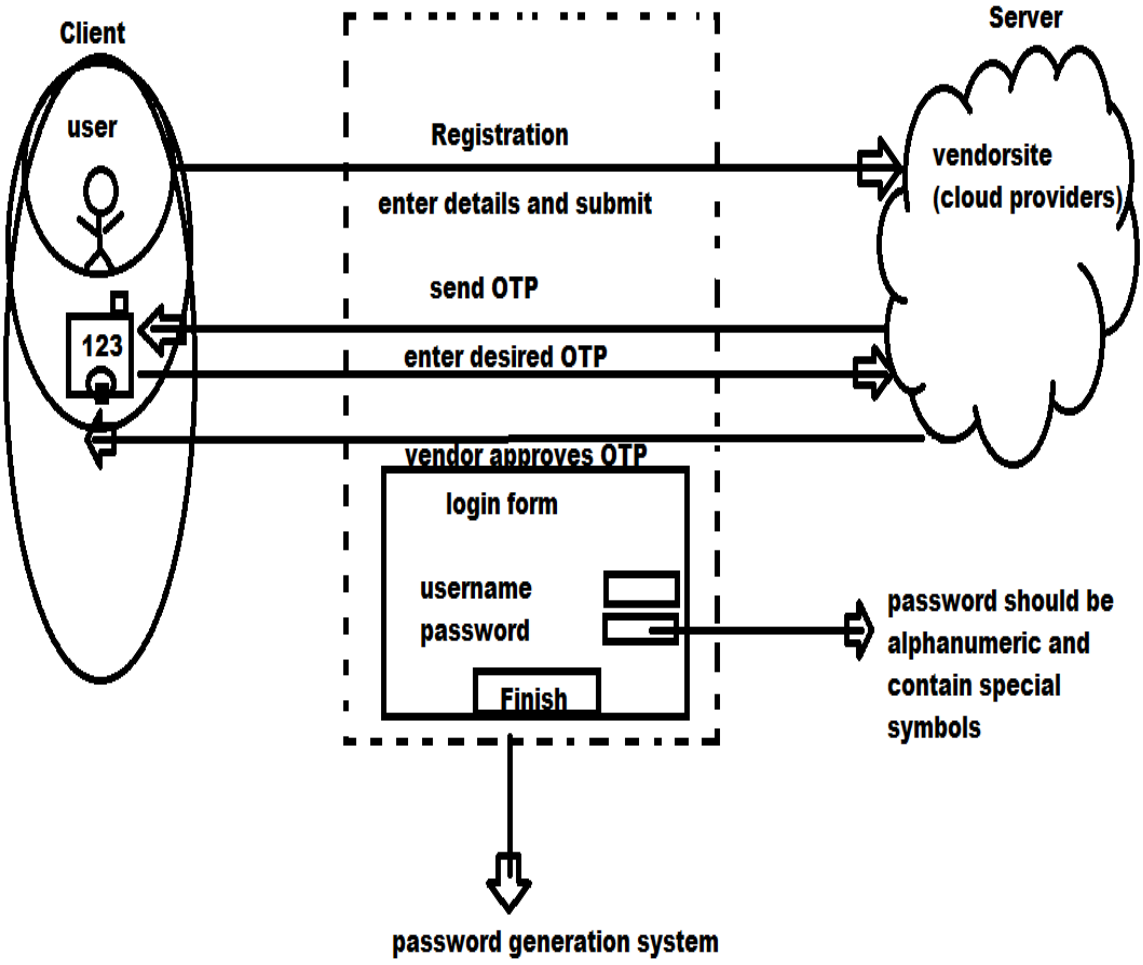

Fig 1: Password authentication Scheme

3.1. Algorithm for password generation

Input: -> user details, name, ID, type of services wants to subscribe, signature.

Password-gen-algo (client, password generation, server)

Output: -> multi-password

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Issue 2, February 2017

-> Initialize client as x, password-generation say y and server as z.

-> Enter user details (x, y, and z)

-> Complete registration process (x, y, and z)

-> Server generates OTP at client devises (x, y, z+1)

// here server gets updated as it has to move to other location for generating OTP//.

->Client enters OTP (x+1, y, z+1)

// here client moves to next page to enter OTP//

->vender approves OTP (x+1, y, z+1)

->login form generated (x+1, y+1, z+1)

// here login credential form is generated //.

->client enters its user name and password according to his/her wish.

->finish the process.

4. CONCLUSION

Cloud security is one of major concerns that need to be addressed. Although cloud computing provides scalable and ease to use services but if data is not kept secure then it is of no use. Cloud standards must be maintained for ensuring authenticity and confidentiality. The paper introduced multi-dimensional password generation technique that is issued to each client before using services. It prevents data from attacking by intruders and untrusted parties.

REFERENCES

[1]. Y, Amanatullah, Ipung H.P., Juliandri A, and Lim C. "Toward cloud computing reference architecture: Cloud service management perspective.". Jakarta: 2013, pp. 1-4, 13-14 Jun. 2013

[2]. X. Suo, Y. Zhu, G. S. Owen, “Graphical passwords: A survey,” in Proc. 21st Annual Computer Security Application. Conf. Dec. 5–9, 2005, pp. 463–472.

[3]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords: Basic results,” in Proc. Human-Comput.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Issue 2, February 2017

Interaction Int., Las Vegas, NV, Jul. 25–27, 2005

[4]. Safiriyu Eludiora1, Olatunde Abiona2,Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde "A User Identity Management Protocol for Cloud Computing Paradigm" appeared in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

[5]. E. Goh, (2003) "Building Secure Indexes for Searching Efficiently on Encrypted Compressed Data", http://eprint.iacr.org/2003/216/

[6]. Yang , Kan; Jia, Xiaohua; Ren, Kui & Bo Zhang, (2013) "DAC-MACS: Effective data access control for multi-authority cloud storage systems", INFOCOM, 2013 Proceedings IEEE , pp 2895 – 2903

[7]. AlZain, M.A.; Soh, B. & E. Pardede, (2013) "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", Journal of Software, Vol. 8, No. 5, May 2013

[8]. Ruj, S.; Stojmenovic, M. & A.Nayak, (2014) "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds), IEEE Transactions on Parallel and Distributed Systems, pp 384 – 394

[9]. Gurudatt Kulkarni et al, "Cloud Security Challenges'', 7th International Conference on telecommunication systems, Services and Applications(TSSA),IEEE,2012

[10]. Rajnish Choubey et al., "A Survey on Cloud Computing Security, Challenges, Threats'', International Journal on computer Science and Engineering (IJCSE) 2011