JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Method To Enhance the Authentication and Access Technique for Password Generation and security using Cloud Services

Amrit lal patel **Dr. Vijay Anand** **Dr. Sunita Gond**

amritpate@gmail.com sunitagond11g@gmail.com

MADHYANCHAL PROFESSIONAL UNIVERSITY, BHOPAL

Abstract

Cloud ssecurity sstandards describes various standards required to take precaution measures in cloud computing in order to prevent attacks and it also governs various policies of cloud computing for security without compromising reliability and performance in the environment. Network involves many attacks such as cconnection aavailability, Denial of Service (DoS), DDoS, flooding attack, etc. Various issues that affect privacy of user information and data storage also related to data related security issues including data migration, integrity, confidentiality, and data warehousing. An innovative novel approach is required to generate password that is OTP based for enhancing the security in cloud environment. Reduction of various unexpected attack like brute force attack etc. and multidimensional password reduces the probability of the hacker, OTP with images enhances security of the transactions. Different password used for different transactions, lesser the intrusion probability. We here present and evaluate the effectiveness and general counter measures for cloud security attacks including intrusion detection systems, autonomous systems, and identity management systems.

Keywords:

Cloud computing, DoS, OTP, DDoS, Flooding attack.

Introduction

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud computing stores the data and its disseminated resources in the environment, security has become the main obstacle which is hampering the deployment of cloud environments. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party.

In many surveys and researches it is mentioned that security is now the main challenge to be deal within cloud. But without any reservation, Infrastructure-as-a-Service (IaaS) of public cloud, risks highest among all. Several security management standards and measures have been intended to safeguard the cloud system, but nevertheless its security is at a high risk due to the innovative hacking techniques. Research focus on identifying the security threats and issues and their countermeasures independent, low-cost, flexibility and reliability related with cloud computing security.

Literature Review

Mohit Garg [1] introduce a technique of hiding a secret message using text file.This process is basically called as text steganography, but the steganographic technique is slightly different because it uses html file to hide the secret message in this method the secret message is encrypted using play-fair cipher encryption mechanism which convert the message into binary format.

Paul. A. J, Varghese Paul, P. Mythili [2] introduce the encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) are widely used to solve the problem of communication over an insecure channel.

Grover Aman, Narang Winnie [3] proposed 4-D password uses the multifactor authentication consists of biometrics, graphical and textual passwords are embedded in a 4-D password authentication technique.

Richa Chowdhary and Satyakshma Rawat [4] use the one-time password implementation for authenticating services from multiple clouds at once. They elaborate what actually the cloud is and about the use of multi-clouds in organizations. It then investigates the security issues in cloud and finally the one-time password concept. The implementation of this model is then discussed. other file systems prove to be successful in homogeneous clusters but not in heterogeneous cluster environment Query Performance As per [Mert Akdere, 2011].

Proposed Methodology

Various types of cloud environment attack are seen, for this we need strong platform. Here we have a table that shows various IoT malicious flows**.**

#	Name of Dataset	Duration (hrs)	#Packets	#ZeekFlows	Pcap Size	Name
1	CTU-IoT-Malware-Capture-34-1	24	233,000	23,146	121 MB	Mirai
2	CTU-IoT-Malware-Capture-43-1	1	82,000,000	67,321,810	6 GB	Mirai
3	CTU-IoT-Malware-Capture-44-1	2	1,309,000	238	1.7 GB	Mirai
4	CTU-IoT-Malware-Capture-49-1	8	18,000,000	5,410,562	1.3 GB	Mirai
5	CTU-IoT-Malware-Capture-52-1	24	64,000,000	19,781,379	4.6 GB	Mirai
6	CTU-IoT-Malware-Capture-20-1	24	50,000	3,210	3.9 MB	Torii
7	CTU-IoT-Malware-Capture-21-1	24	50,000	3,287	3.9 MB	Torii
8	CTU-IoT-Malware-Capture-42-1	8	24,000	4,427	2.8 MB	Trojan
9	CTU-IoT-Malware-Capture-60-1	24	271,000,000	3,581,029	21 GB	Gagfyt
10	CTU-IoT-Malware-Capture-17-1	24	109,000,000	54,659,864	7.8 GB	Kenjiro
11	CTU-IoT-Malware-Capture-36-1	24	13,000,000	13,645,107	992 MB	Okiru
12	CTU-IoT-Malware-Capture-33-1	24	54,000,000	54,454,592	3.9 GB	Kenjiro
13	CTU-IoT-Malware-Capture-8-1	24	23,000	10,404	2.1 MB	Hakai
14	CTU-IoT-Malware-Capture-35-1	24	46,000,000	10,447,796	3.6G	Mirai
15	CTU-IoT-Malware-Capture-48-1	24	13,000,000	3,394,347	1.2G	Mirai
16	CTU-IoT-Malware-Capture-39-1	7	73,000,000	73,568,982	5.3GB	IRCBot
17	CTU-IoT-Malware-Capture-7-1	24	11,000,000	11,454,723	897 MB	Linux,Mirai
18	CTU-IoT-Malware-Capture-9-1	24	6,437,000	6,378,294	472 MB	Linux.Hajime
19	CTU-IoT-Malware-Capture-3-1	36	496,000	156,104	56 MB	Muhstik
20	CTU-IoT-Malware-Capture-1-1	112	1,686,000	1,008,749	140 MB	Hide and Seek

We have another table that shows bbreakdown of Application Layer Protocols as detected on the Malicious Scenarios.

#	Name of Dataset	HTTP	DNS	DHCP	TELNET	SSL	SSH	IRC	Not recognized by Zeek	Name
1	CTU-IoT-Malware-Capture-34-1	12	192	2	-	-	-	1,641	21,298	Mirai
2	CTU-IoT-Malware-Capture-43-1	16	204	-	-	-	-	-	67,321,589	Mirai
3	CTU-IoT-Malware-Capture-44-1	11	-	-	-	-	-	-	226	Mirai
4	CTU-IoT-Malware-Capture-49-1	19	6	1	-	-	-	-	5,410,535	Mirai
5	CTU-IoT-Malware-Capture-52-1	14	4	1	-	-	-	-	19,781,359	Mirai
6	CTU-IoT-Malware-Capture-20-1	-	592	-	-	-	-	-	2,617	Torii
7	CTU-IoT-Malware-Capture-21-1	-	1,924	-	-	-	-	-	1,362	Torii
8	CTU-IoT-Malware-Capture-42-1	33	1,680	1	-	2	-	-	2,710	Trojan
9	CTU-IoT-Malware-Capture-60-1	-	-	2	-	-	-	-	3,581,026	Gagfyt
10	CTU-IoT-Malware-Capture-17-1	4	11,902	-	-	-	-	-	54,647,949	Kenjiro
11	CTU-IoT-Malware-Capture-36-1	-	751	2	-	-	-	-	13,644,345	Okiru
12	CTU-IoT-Malware-Capture-33-1	228	80	2	-	-	-	-	54,454,281	Kenjiro
13	CTU-IoT-Malware-Capture-8-1	-	-	-	-	-	-	-	10,403	Hakai
14	CTU-IoT-Malware-Capture-35-1	36	1,479	2	-	9	-	-	10,446,261	Mirai
15	CTU-IoT-Malware-Capture-48-1	11	2	-	-	-	-	-	3,394,325	Mirai
16	CTU-IoT-Malware-Capture-39-1	14	2,308	-	-	6	538	914	73,565,201	IRCBot
17	CTU-IoT-Malware-Capture-7-1	-	7	1	-	-	-	-	11,454,706	Linux,Mirai
18	CTU-IoT-Malware-Capture-9-1	55	1,162	-	-	-	-	-	6,377,076	Linux.Hajime
19	CTU-IoT-Malware-Capture-3-1	-	1	3	-	-	5,898	6	150,195	Muhstik
20	CTU-IoT-Malware-Capture-1-1	3,238	1	1	-		-	-	1,005,507	Hide and Seek

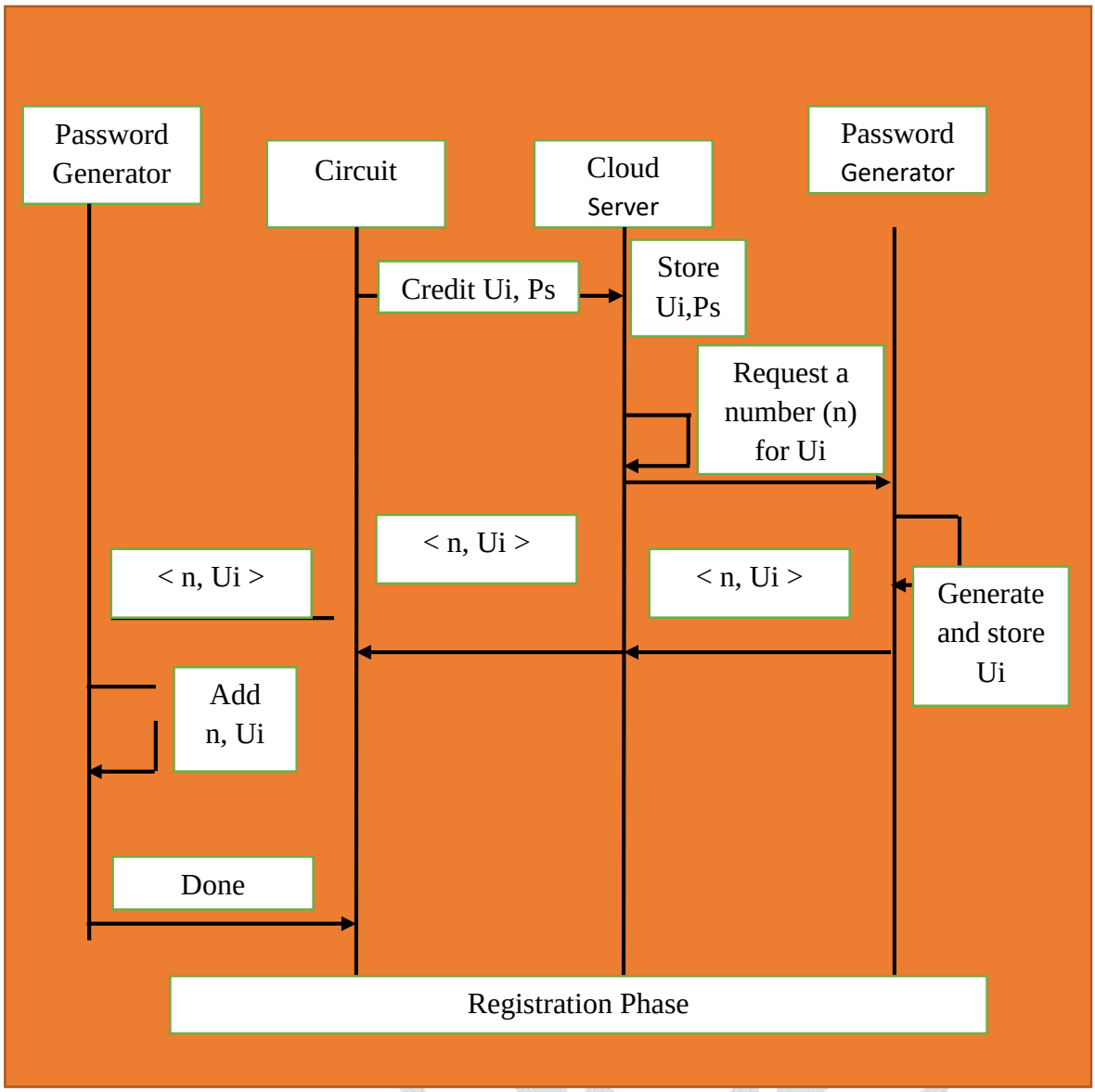
An innovative novel approach is required to generate password that are OTP based for enhancing the security in cloud environment.

Step1: After inserting userid (Ui) and Password (Ps), Cloud server verifies the authenticity of user (Ui, Ps)

Step2: At the time login request received by cloud server, it immediately send a message to user for OTP generation.

Step3: For every request OTP (a new key generated every time) and a symmetric value that is available with user and one copy on cloud server.

Step 4: Authentication check after matching of same value of OTP with user and cloud server.



Examples: -

16	14	10	8	6	5	12	13	1	4	2
0	1	2	3	4	5	6	7	8	9	10

i) Use remainder method (Let here total no of slots are 0-10=11) so, modulus use 11 every time to calculate value of pin.

let's 54 % 11=10

on 10^{th} we get 02 so pin is 1002

ii) let's 17 % 11=06

on 6^{th} we get 12 so pin is | 0612 |

If the calculated value is not having slot free than try for next immediate free slot. In the similar way for every transaction value used for modules division are different and not easy to guess by everyone, so the proposed methodology is boost up the system and make system secure.

Expected Outcome

- Reduction of various unexpected attack like brute force attack.
- Multidimensional password reduces the probability of the hacker.
- OTP with images enhances security of the transactions
- Different password used for different transactions, lesser the intrusion probability.

Conclusion

Cloud ssecurity sstandards describes various standards required to take precaution measures in cloud computing in order to prevent attacks and it also governs various policies of cloud computing for security without compromising reliability and performance in the environment. Network involves many attacks such as cconnection aavailability, Denial of Service (DoS), DDoS, flooding attack, etc. Various issues that affect privacy of user information and data storage also related to data related security issues including data migration, integrity, confidentiality, and data warehousing.

We here present and evaluate the effectiveness and general counter measures for cloud security attacks including intrusion detection systems, autonomous systems, and identity management systems.

Parameters that we are going to improve are: -

1. Authentication level
2. Password creation complexity
3. Less Brute force attack

Compatibility with the devices

References

[1] Jyoti chaurasia, Om Prakash Karada, "Three-Dimensional Password Generation Technique for Accessing Cloud Services", International Journal on Advanced Computer Theory and Engineering (IJACTE) ISSN (Print): 2319 – 2526, Volume-2, Issue-4,2013.

[2] Dinesha H A and Dr. V. K. Agrawal, "Multi-dimensional password generation techniques for accessing cloud services", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.3, June 2012DOI: 10.5121/ijccsa.2012.2304 31.

[3] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", DOI 10.1109/TPDS.2014.2308218, IEEE Transactions on Parallel and Distributed Systems.

[5] Deepak G, Dr. Pradeep. B. S, Shreyas Srinath, "Dynamic Key Generation Algorithm for User Authentication at Mobile Cloud Environment" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358 Volume 3 Issue 7, July 2014 www.ijsr.net.

[6] Monika Agarwal, "Text steganographic approaches: A comparison", International Journal of Network Security & Its Applications (IJNSA)", Vol.5, No.1, January 2013 DOI: 10.5121/ijnsa.2013.5107 91.

[7] Mohit Garg, "A Novel Text Steganography Technique Based on HTML", International Journal of Advanced Science and Technology Vol. 35, October, 2011 129

[8] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, "Secure Authentication with 3D Password", Volume 2, Issue 2, page no. International Journal of Engineering Science and Innovative Technology (IJESIT) March 2013

[9] Paul. A.J*, Varghese Paul, P. Mythili, "A fast and secure encryption algorithm for message communication", International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007),

[10] Grover Aman, Narang Winnie,"4-D password: Stenting the authentication scene", volume 3 Issue 10, International Journal of Scientific and Research Publications, October- 2012, ISSN 2229-5518

[11] Richa Chowdhary Satyakshma Rawat, "One Time Password for Multi-Cloud Environment" Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com

[12]. S.C.Wang,M.L,Chiang,K.Q.Yan,S.S.Wang,S.H.T sai,"A New Group Key Authentication protocol in an insecure cloud computing environment", in International conference on Advanced Information Technologies(AIT),2011.

[13]. D.Ranjith,.Srinivasan," Identity Security Using Authentication and Authorization in Cloud Computing "in International Journal of Computer & Organization Trends,Vol.3,Issue 4,May 2013,ISSN:2249-2593

14]. Umer Khalid,Misbah Irum,Muhammad Awais Shibli,"Cloud based Secure and Privacy Enhanced Authentication and Authorization Protocol", in Elsevier on ScienceDirect,Vol.22,2013,DOI:10.1016/j. procs. 2013.09.149, pp:680-688.

[15]. Ahmed Almulhem,"A Graphical Password Authentication System", in IEEE explore on ResearchGate, Apr 2011.

[16]. Jun Hu, Lei chen, Yunhua wang, Shi-hong chen,"Data Security Access Control Model of Cloud Computing", in IEEE explores International Conference on Computer Sciences and Applications,2013, DOI:10.1109/CSA.2013.15.

[17]. Younis A.Younis,Kashif kifayat,Madjd merabti,"An Access Control Model for Cloud Computing", in Elsevier,Vol.19,Issue 1,Feb 2014.

[18]. Vishal paranjape,Vimmi pandey,"An Improved Authentication Technique with OTP in Cloud Computing", in International Journal of Scientific Research in Computer Science and Engineering,Vol.1,Issue 3,June 2013,EISSn:2320-7639.

[19]. Iehab AL Rassan,Hanan Al Shaher,"Secure Mobile Cloud Computing using Biometric Authentication", in IEEE explore on Academy and Industry Research Collaboration Center(AIRCC),Vol.5,Issue 6,pp:41.

[20]. D.chandramohan,.Vengattaraman,D.Rajaguru,P. Dhavachelven"A New Privacy Preserving Technique for Cloud Service User Endorsement using Multi-agents", in ScienceDirect on Journal of King Saud University-Computer and Information Sciences,Vol.28,Issue 1,Jan 2016,pp:37-54DOI:10.1016/j.jksuci.2014.06.018.

[21]. Nitin nagar,Pradeep K.Jatav,"A Secure Authenticate Framework for Cloud Computing Environment", in Google Scholar on International Journal of Advanced Computer Research(IJACR),Vol.4,No.14,2014,pp:266-271.