Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 6, Issue, 4, pp.3739-3743, April, 2015

International Journal of Recent Scientific Research

RESEARCH ARTICLE

PATTERN BASED USER AUTHENTICATION FOR SECURE CLOUD ACCESS AND STORAGE

Prafull S. Kadam and Pramod A. Jadhav

Bharati Vidyapeeth University, Collage of Engineering, Pune

ARTICLE INFO

Article History:

Received 14th, March, 2015
Received in revised form 23th, March, 2015
Accepted 13th, April, 2015
Published online 28th, April, 2015

Key words:

Logging, pattern analysis, outlier, user profiling, user log global, session key, session timing, local user log , key stroke pattern, keystroke amplitude, server authorizer, and auditing.

ABSTRACT

Cloud system environment ensures that user can use highly extensive drivable services resource over the network as and when required. The main aim of the cloud services is the dealing out of users' information is carried out remotely. The user does not own or operate these remote machines. However users always worried about their confidential data, it might be compromised when they use this new environment. This limitation can turn into hindrance to the extensive use of cloud services resource. Paper presents to attend this problem, by using a new highly distributed information accountability cloud bundle. This cloud bundle lets user monitoring to the real usage of the user information inside cloud. This proposed cloud bundle has an object-and domain centered steps which we can use to club the logging method with users' information and policies. This proposed cloud bundle uses the jar programmable capabilities for creating active and roaming object. It also ensures that when anyone accesses the users' data, authentication and automated logging is carried out locally to the jars. In order to make the user's control strong, we can give distributed auditing methods. This proposed cloud bundle also ensures extensive experimental studies to demonstrate that the proposed steps are efficient and effective.

INTRODUCTION

Cloud computing is biggest rising technology in today's world of ecommerce which insist to make available scalable access and security. Users are able to access cloud storage when they have logged in with authority, there is no need to worrying about information, not necessary to confirm its reliability. Cloud computing is nothing but relief of computing services, on the Internet. Now they understand it, many users use cloud computing services for their personal needs. Example: citizens make use of social networking websites or mail and those are cloud services. Now days organizations are paying attention in cloud computing. Cloud computing can considerably condense the price and difficulty of owning and handling computers and network's. When organization use's a cloud source, it doesn't require paying out money on Information Technology Infrastructure.

Current system

In order to address the cloud environment. old cloud system relay on SLA agreement and agent log metadata to monitor and audit the producer and consumer usage as well other resource action ,we proposed pattern based approached to provide user profiling for harden security system.

Existing problems in current systems

First, the agent cloud service provider (acsp) can outsource this information regulation to other entities inside cloud. Those other entities can sub-association the tasks, to other entities further.

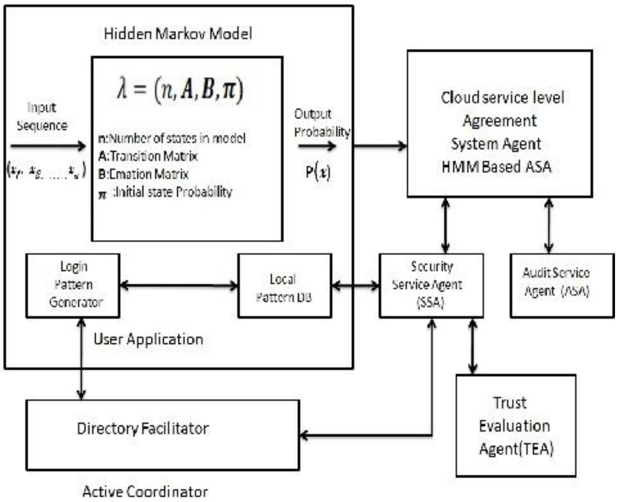
Second, entities can join and leave the cloud as per their flexibility. so the data regulation in the cloud is done in a hierarchical and dynamic service chain. This type of processing is not done in conventional environments.

Proposed system with keystroke enhance model

This proposed framework has the following approach, called Cloud Information Accountability (HMM BASED ASA) framework. This framework is based on the idea of information accountability. This approach is different from privacy protection. This framework focuses on keeping the data usage transparent and tractable. This proposed HMM BASED ASA

Corresponding author:* **Prafull S. Kadam
Bharati Vidyapeeth University, Collage of Engineering, Pune

framework has an end-to end accountability that is available in a highly distributed manner. The HMM BASED ASA framework can maintaining lightweight and powerful accountability covering access control, usage control and authentication. Using the HMM BASED ASA ensure the that Tracking whether SLA agreements are confirmed, and whether Access and usage control policies are being implemented for benefit for the data owners.

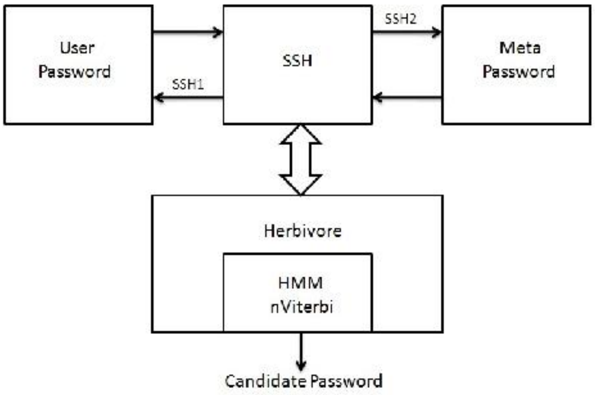

Hidden Markov Model
$\lambda = (n, A, B, \pi)$
Input Sequence
$(x_1, x_2, \ldots, x_n)$
n:Number of states in model
A:Transition Matrix
B:Emation Matrix
π :Initial state Probability
Output Probability
P(x)
Cloud service level Agreement System Agent HMM Based ASA
Login Pattern Generator
Local Pattern DB
Security Service Agent (SSA)
Audit Service Agent (ASA)
User Application
Directory Facilitator
Trust Evaluation Agent(TEA)
Active Coordinator

Under the accountability feature, two modes can be possible: push mode and pull mode. In the push mode, logs are sent periodically to the data owner or stakeholder. In the pull mode, more than party can retrieve log data when it is required.

Main contributions

We propose a novel automatic and enforceable logging method in the cloud. Paper present extensive architecture, which is platform-independent and highly distributed. It does not need a devoted verification or storage system to authenticate.

Novel keystroke pattern generator method for local SLA



We must arrange the consumer passwords in decreasing order of the weighting probability pr *q*, *y*, and as such we must record the position of the consumer actual signature password in the consumer list in our local DB which synchronize with cloud SLA DB. The position of the password as a percentage. Let us consider where there are a total of *m* possible passwords. If in the ordered consumer list, the consumer actual signature password appears at position *u*, we can assume that the consumer actual signature password appears at the top 100*u m* %. In this manner, we can naturally quantify the effectiveness of our steps.

Move further than traditional access control, where we give a certain amount of usage control for the user's protected information after the receivers gets this data.

These experiments are conducted on a consumer actual signature cloud test bed. The obtained outcome validates the efficiency, scalability and granularity of the proposed model. Proposed model also provides a full security analysis that reflects the dependability and potential by using local pattern based security as a preliminary step for global authentication.

Optimization for Long Character Sequences

Viterbi algorithm group the frequent set of pattern in cluster format for selecting probable chain. So to learn the weight model and to reduce the buffer usage of the algorithm, we break the Keystroke information of the password into Cluster containing 3 or 4 latency intervals. Each segment is used to form a HMM and then finally the result is combined from different segments to form the candidate password ordering.

Algorithm given below work on given mathematical model

$$p(x) = \sum_{y} p(x, y) = \sum_{y} \prod_{t=1}^{T} p(y_t | y_{t-1})\, p(x_t | y_t)$$

Algorithm

A. ***Suppose to classify set of password sequences***

1. **Initiate input Sequences** N user class of sequences: starts and ends with alpha numeric value
2. Now assign respective class labels ULabelclass[] output Labels class as follows
   Sequences A-z, 1-9 are from class user1:,
   Sequences A-z, 1-9 are from class user2:,
   Sequences A-z, 1-9 are from class user3:
3. Algorithm use a single protocol for all inner models,
   Protocol FwdHmm = new FwdHmm (states: User class);
4. create a hidden Markov classifier with the given Protocol
   HMM Classifier HMMC = new HMM Classifier r(classes: user class, protocol: Fwd Hmm, symbols: password);
5. Apply above steps to teach and learn each of the classified models
   Teach = new HMM Classifier Learn(HMM Classifier,
6. specify alone training options for each classified model:
   M Index => new ViterbiLearning(HMM classifier. Models[M Index])
   Set
   Tolerance = 0.005,
   Iterate until likelihood changes less than 0.005
   Iterations = 0
   Upper limit not greater then

7. Initiate learning process
8. Error = Teach. Run (Password Sequences, UoutputLabels);
9. After training has finished, Will get label sequences

B. Discrete approach for auditing

Forward mode

The forward mode refers to logs that are sending at regular intervals the information owner or stakeholder.

Backward mode

In the backward mode the users (or a new certified party) can fetch the logs when required.

C. Techniques using in logging and auditing

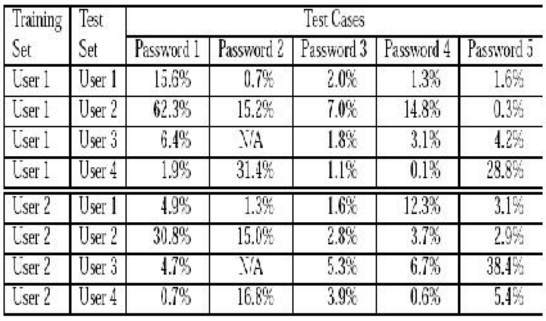
1. To getting feel of the active nature of the cloud, the logging should be decentralized. Also log files and the corresponding data being controlled should be tightly bounded. There is need of negligible infrastructural support from any of the server.
2. This logs must record each access to the user's information properly and by design. Integrated techniques are needed that help authenticate the state that allow to use information and confirm and evidence that the real operations that are carried out on the information. The time this activity was carried out should also be recorded.
3. Log files must be consistent and tamper evidence. Malicious parties must not be able to illegal insert, delete or modify the log files. There must also be recovery methods to repair damage log files that are occurred due to technical problems.
4. The information owners must be mailed the log files from time to time to notify them of the present usage of their information. Also prominently, the information owners must be able to retrieve the log files by their information owners, when required apart from the position at their files are stored. There is no specific time.
5. This intent technique should not intrusively keep track of records recipient's systems. There must not be important communication and estimation overheads, as these will hold back its probability and acceptance at daily use.
6. Key component of HMM BASED ASA:

The two major components of the HMM BASED ASA are the logger, and the log mediator who brings thing into harmonious agreement with another. The logger is robustly bound with user information (which having distinct or numerous information entities). The important job of logger include automatically logging allow to use to information entities that it containing; encrypt the log documentation by using the content owner's public key, and once in a while sending them towards log harmonizer. The logger should be configured to make sure that allow using and control policies related with the information usage are privileged. Example, Information owner can require that user x will not modify the data but is only allowed to view. Even after the information it is downloaded with the help of user x, this logger will manage the information access. The middle module which gives admittance to the user access to logger files, that formed by log harmonizer. The log harmonizer is responsible for auditing purpose.

Investigational outcome for password intervention for multiple users

One latent limitation in our simulations is that consumer actual signature world assaulter may not be able to acquire the training information from the sufferer for the arithmetical examination which present in our experiments. When we disagree after that is improbable to pose an effectual protection against timing attacks: there are different ways that attacker receiving the guidance that information necessary to the attack. One of the easy conditions is that the attacker can without trouble get his own typing information, or the typing information of a partner. So, it is essential to estimate how well, the password intervention techniques execute while using one user's typing statistics to infer passwords typed by another user.

In this research, we collected the typing statistics of two person, user1 and user2. An exciting outcome is that 75% of the character pairs getting same latency to type for both two users: we can say that, the dissimilarity between the average latencies of the two persons for such character pairs is slighter than its standard deviation. Correspondingly, the plain timing characteristics reported, key pairs typed with interchange pairs tend to have minor inter-keystroke latency than key pairs typed with the similar hand that are observed, which fundamentally user-independent. This suggests that typing statistics having huge element that is frequent across a wide user residents and so it can be broken by attackers even we doesn't provide any training information from the sufferer.



Training Set	Test Set	Test Cases				
		Password 1	Password 2	Password 3	Password 4	Password 5
User 1	User 1	15.6%	0.7%	2.0%	1.3%	1.6%
User 1	User 2	62.3%	15.2%	7.0%	14.8%	0.3%
User 1	User 3	6.4%	N/A	1.8%	3.1%	4.2%
User 1	User 4	1.9%	31.4%	1.1%	0.1%	28.8%
User 2	User 1	4.9%	1.3%	1.6%	12.3%	3.1%
User 2	User 2	30.8%	15.0%	2.8%	3.7%	2.9%
User 2	User 3	4.7%	N/A	5.3%	6.7%	38.4%
User 2	User 4	0.7%	16.8%	3.9%	0.6%	5.4%

Success rates for password inference with multiple users. The numbers are the percentage of the search space the attacker has to search before he finds the right password.

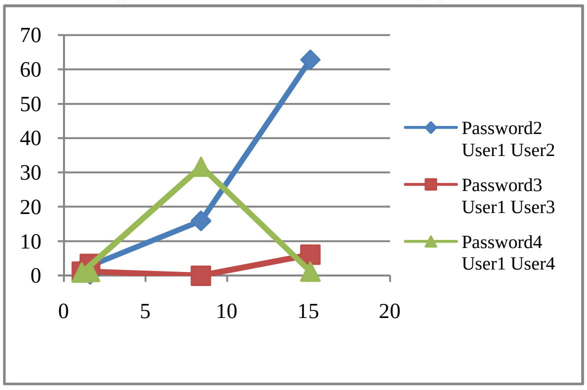


Chart1 High probabilistic Pattern

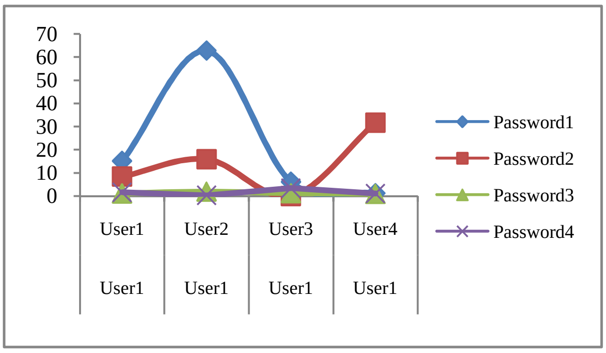


Chart2 Pattern Recognition For User

CONCLUSION

In stateless cloud computing environment every resource and its consumer are hardenly long for cloud auditability and its accountability purpose, no sequence as well learned history as a log with not use for any agreement. It causes no future predictability for resource and its consumer acquires process, also may highly impact on its maintenance cost. There for we purpose probable pattern matching algorithm in terms of HMM to calculate and predict user level authentication on login process even after cloud log history getting generated ,password pattern may authenticate duplicate login in advance as well as learned history will be used for auditability of cloud.

Future Scope

User based pattern logger is effective technique for high security as well as large data for user profiling activity monitoring, in terms of cloud auditing if we extend the further functionality related to consumer and producer pattern based , then consumer can do blind belief on cloud environment for their expensive operation ,the operation include ,data communication ,service operation, storage, usage operation and so on, HMM based light model can apply in future for harden reliability and security.

References

1. “An Effective Clustering-Based Approach for Outlier Detection” by Moh‟Belal Al- Zoubi *European Journal of Scientific Research* Vol.28 No.2 (2009).
2. “Outlier Detection using Clustering Methods: a Data Cleaning Application” by Loureiro,A., L. Torgo and C. Soares, 2004 in Proceedings of KDNet Symposium on Knowledge-based Systems for the Public Sector. Bonn, Germany.
3. A New Hybridized K-Means Clustering Based Outlier Detection Technique For Effective Data Mining
4. Analysis. Proceedings of the Second International Network Conference (INC): pp. 263-ISBN 1 84102 066 4, Plymouth, UK, 03-06 July, 2000.
5. Balakrishnan S, Saranya G, *et al.* (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, *International Journal of Computer Science and Technology*, vol 2(2), 397–400.
6. Baldwin, S. Shiu and Y. Beres, “Auditing in shared distributed virtualized environments,” HP Technical Reports, 2008.
7. Cloud Security Alliance, “Top Threats to Cloud Computing (V1.0),” 2010; https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
8. Design and Evaluation of a Pressure Based Typing Biometric Authentication System MJE Salami, Wasil Eltahir and Hashimah Ali International Islamic University Malaysia (IIUM) Malaysia ;Araujo, L.C.F.; Sucupira, L.H.R.; Lizarraga, M.G.; Ling, L.L. &Yabu-Uti, J.B.T. (2005).
9. H.S.Behera Abhishek Ghosh. Sipak ku. Mishra Computer Science and Engineering, Computer Science and Engineering, Computer Science and Engineering VSSUT, Burla Odisha, India VSSUT, Burla, Odisha, India. VSSUT, Burla, Odisha, India.
10. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com.
11. M. Vouk, “Cloud computing—Issues, research and implementations,” Proc. 30th International Conference on Information Technology Interfaces, 2008 (ITI 2008) IEEE, 2008, pp. 31-40.
12. Oxford University Press, “Concise Oxford English Dictionary,” Retrieved December, vol. 5, 2005, pp. 2005.
13. P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.
14. Recognition, Volume 3 pages 430 – 433, Cambridge, UK, August 2004. ||Volume||2|| Issue|| 7|| Pages 1185-1194|||July-2014|| ISSN (e): 2321- 7545.
15. Robust Outlier Detection Technique in Data Mining: A Univariate Approach. Singh Vijendra and Pathak Shivani Faculty of Engineering and TechnologyMody Institute of Technology and Science Lakshmangarh, Sikar, Rajasthan, India.
16. S. Pearson and A. Charles worth, “Accountability as a way forward for privacy protection in the cloud,” Cloud Computing, 2009, pp. 131-144.
17. Security using Fusion of Keystroke and Mouse Dynamics (Result Paper)Authors Yogesh R.Nagargoje1, Dr.Santosh S.Lomte2, Prof.Rajesh.A.Auti3, Anil H.Rokade *International Journal Of Scientific Research And Education.*
18. Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm Miss. Nupoor M. Yawale Prof. V. B. Gadichha M.E. Second year CSE P R Patil COET P R Patil COET, Amravati. INDIA. Amravati. INDIA. *International Journal of Advanced Research in Computer Science and Software Engineering Research* Paper Available online at: www.ijarcsse.com.
19. Trust Cloud: A Framework for Accountability and Trust in Cloud Computing Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, HP Laboratories, HPL-2011-38.

20. US House of Representatives, The Best Practices Act of 2010 and Other Privacy Legislation, T. Sub-Committee on Commerce, and Consumer Protection, 2010.
21. Using Third Party Auditor for Cloud Data Security: A Review; Ashish Bhagat Ravi Kant Sahu Department Of Computer Science & Engineering School of Computer Engineering, Lovely Professional University, India Lovely Professional University, India.
22. www.ijcat.com;

How to cite this article:

Prafull S. Kadam ., Pattern Based User Authentication For Secure Cloud Access And Storage. *International Journal of Recent Scientific Research Vol. 6, Issue, 4, pp.3739-3743, April, 2015*

****