INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2454 - 2460
RECEIVED : 20.05.2017 PUBLISHED : 09.06.2017
June 09, 2017

ENHANCED CLOUD ARMOUR FOR DEVELOPING TRUST MANAGEMENT

[1]Sayana Abraham, [2]Mr. T Sivakumar,
[1]PG Scholar, Department of computer science and engineering, Maharaja Institute of Technology, Coimbatore,
[2]Assistant Professor, Department of Computer science and engineering,
Maharaja Institute of Technology, Coimbatore.

1. INTRODUCTION

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. In the New age communication cloud has been introduced. There are various services Available in the cloud server like (IaaS) – Infrastructure as a service, (PaaS)- Platform as a service, (SaaS) – Sofware as a service. From these services for security purpose (TaaS) – Trust as a service has been implemented. But we need more improvement in the TaaS. The problem facing in all IT companies are hacking, through hacking a web server the company's total technology can be stolen from the database. Still this problem is in all IT Companies. And the most important problem is trust. Also confidential code team should be monitor and should make a efficient security ring. In order to overcome these problems in this project we introducing a secured DNS with enhanced database which supports on cloud mail server. Also we introducing a procedure based security methodology called as instruction detection system (IDS) with three types of synchronization: Namely, IP Synchronization, Data Synchronization and Time Synchronization. So that the main object is to create privacy preservation for the confidential database the proposed architecture implements the real world anonymous database by implementing the generalization and suppression. Along with Gaussian mixture and keystroke for secured login. Along with colour code has been used. The efficiency and security of data can be achieved by maintaining single database with specific access rights. With the action performed with IDS with ESMTP in Anonymous and Confidential Databases.

Keywords : Trust as a service (TaaS), Privacy, Preservation, Intrusion Detection System (IDS), User Rights, Synchronizations, SMTP, Mail server, Gaussian mixture and keystroke for secured login.

2. RELATED WORKS

We begin this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations. We then address those limitations by proposing more rigorous mechanisms based on evidence, attribute certification, and validation, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the cloud [1]. The Internet cloud works as a service factory built around virtualized data centres. Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service oriented platform using virtual server clusters at data centres [2]. As the business market is growing rapidly with new providers entering the market, cloud providers will increasingly compete for customers by providing services with similar functionality. However, there can be huge differences regarding the provided quality level of those services. Such a competitive market needs means to reliably assess the quality level of the service

providers [3]. SOC (service-oriented computing) represents a new generation of distributed computing framework for applications development by means of the composition of services. The visionary promise of SOC is a world-scale network of loosely coupled services that can be assembled with little effort in agile applications that may span organizations and computing platforms [4].

3. METHODOLOGY

Initially SMTP server will be created. Through the organization creation the SMTP architecture will be accessed. This application Includes various methodology which includes various synchronization methods. Security is a critical issue in mail server. In most of the previous protocols security is an added layer above the routing protocol. We propose a Trust Aware Routing Protocol for secure-trusted routing for mail server and for its functionalities. In TARP, security is inherently built into the routing protocol where each node evaluates the trust level of its neighbours based on a set of attributes and determines the route based on these attributes.

The objective of this research is to implement privacy and preservation. Our method will provides admin in a comfortable zone to maintain security. Admin will be more privilege person in this application. Admin can provide user rights to the user through customizing their Compose, inbox and sent times.

GAUSSIAN MIXTURE AND KEYSTROKE

This method has been used while employees sign up. Another method used here for security is keystroke logging. This allows only the right user to login at the right time. It is the action of tracking the keys struck on a keyboard, so that the person using the keyboard is unaware that their actions are being monitored. Whenever a user is created, the keystroke time of typing his/her password should be noted. When a user logins to send an email, the keystroke time for typing his/her password should matches with the time that is generated in the user creation. So this will provides a well security for the user's id and password from hackers. The keystroke patterns produced during typing have been shown to be unique biometric signatures. Therefore, these patterns can be used as digital signatures to verify the identity of computer users remotely over the internet or locally at a specific workstation. In particular, keystroke recognition can enhance the username and password security model by monitoring the way that these strings are typed. To this end, this paper proposes a novel up-up keystroke latency(UUKL)feature and compares its performance with existing feature and compares its performance with existing features using a Gaussian mixture model(GMM)-based verification system that utilizes an adaptive and user-specific threshold based on the leave-one-out method(LOOM). The results show that the UUKL feature significantly outperforms the commonly used key hold-down time (KD) and down-down keystroke latency (DDKL) features. Overall, the inclusion of the UUKL feature led to an equal error rate (EER)of 4.4% based on a database of 41 users, which is a 2.1% improvement as compared to the existing features. Comprehensive results are also presented for a two-stage authentication system that has shown significant benefits. Lastly, due to many inconsistencies in previous works, a formal keystroke protocol is recommended that consolidates a number of parameters concerning how to improve performance, reliability, and accuracy of keystroke-recognition systems.

4. COLOUR CODE

Colour cryptography is one of the most important security technologies which used to secure the client server authentication, data transaction process and the data itself. As the time and challenge growth, the cryptography also grows up with variety of encryption techniques and algorithms. Among the algorithms, one of the most popular is the colour code encryption. This project concentrates on the study of the PKI concept generally and colour code encryption methods specifically. Furthermore, through this project we can develop the prototype for instant client server check using Java Script. The development process follows the seven systematic phases of system development life cycle. At the end of the development, the prototype of the application is come out readily to be tested. The prototype only covers the transmitting and receiving phases between two parties (client and server).

SYNCHRONIZATION METHODS

IP Synchronization

An IP address has three or four octets (parts). It cannot have a number above 255 in any of its octets. All the octets need to have numbers between 0 and 255. For example, 209.20.5 or 216.222.8.131. The former will include the entire IP range from 209.20.5.0-209.20.5.255. The latter (216.222.8.131) is an address within a IP range. Some Internet services use the source address of the client's computer as a form of authentication. These systems keep track of the Internet Protocol (IP) address that an end user used the last time that user accessed the site and try to determine if the user is legitimate. When that same user accesses the site from a different source IP address, the site asks for further authentication to revalidate the client's computer. This system will allow only the synchronized IP address only. In case the user trying to access the mail sever from the another IP will comes under monitoring zone

Data Synchronization

Most of the mail servers have a storage limit that you cannot exceed. It can vary from one server to another. In the proposed method there is no fixed method for data synchronization. Admin can provide various data limits to various users. When the actual number of query requests is less than the amount set in max worker threads, one thread handles each query request, if the actual number of query request exceeds the amount set in max worker threads, SQL Server pools the worker threads so that the next available worker thread can handle the request. So the data will be restricted. In case of the user will be exceeding the limit, the user will be monitored in the trust level method. All the data will be converted into kilo bytes during the time of upload.

MB x KB / 1024 = y MB (where x = your KB and y = result in MB) we have MB and what to find the related KB x MB * 1024 = y KB has been used

Time Synchronization

Access start time and end time that spans across 12:00 AM on a specified day results in the user having access until the next day, even if the access day is not explicitly configured.

id | Emp ID | login_time | logout_time

1 | 12 |'2017-02-20 11:20:20' | '2017-02-20 12:10:00'

2 | 13 |'2017-02-20 11:25:20' | '2017-02-20 12:20:00'

3 | 12 |'2017-02-20 13:20:20' | '2017-02-20 13:50:00'

4 | 13 |'2017-02-20 12:30:20' | '2017-02-20 12:50:00'

5 | 13 |'2017-02-20 13:10:20' | '2017-02-20 14:20:00'

The above given timeline details enables to configure time-based restrictions for user access to log in to their mail server. This is useful for restricting the time and duration of user logins for all users belonging to the organization. we can specify the days of the week when users can log in, the access start time, and the access end time.

ALGORITHM IMPLEMENTATION

INITIALIZATION:

IP – Internet protocol synchronization

DT - Date synchronization

TM – Time Synchronization

M – Mail

TR – Trust

ALGORITHM PROCESS

Start Process

User login from SMTP

DateTime DateTimeDiff (Mail M)

Get system date/time in SysDT

if (Received Filed is present in M) do

RecentRecDT=0

while (IP,DT, TM (M)) do (On condition)

Get date/time from Received Field in RecDT

if (RecentRecDT < RecDT) then RecentRecDT= RecDT

Calculate IP,DT, TM difference between SysDT and RecentRecDT in DTDiff

Return DTDiff

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2454 - 2460
RECEIVED : 20.05.2017 PUBLISHED : 09.06.2017
June 09, 2017

else if (Resent Filed is present in M) do

RecentResDT=0

while (EOF (M)) do

Get date/time from Resent Field in ResDT

if (RecentResDT < ResDT) then RecentResDT= ResDT

Calculate date/time difference between SysDTand RecentResDT in DTDiff

Return DTDiff else Get date/time from Send Date Filed in SenDT

Calculate date/time difference between SysDT and SenDT in DTDiff

Return DTDiff

Suggest trust

Stop Process

5. RESULT AND DISCUSSION

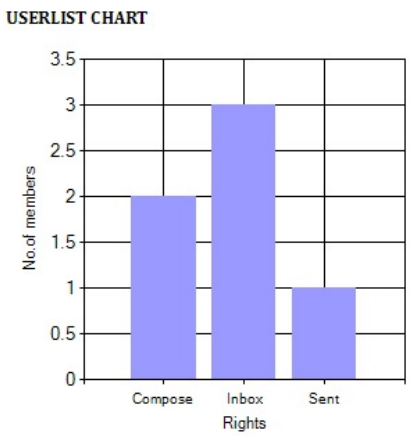

Fig 1. User Rights Chart

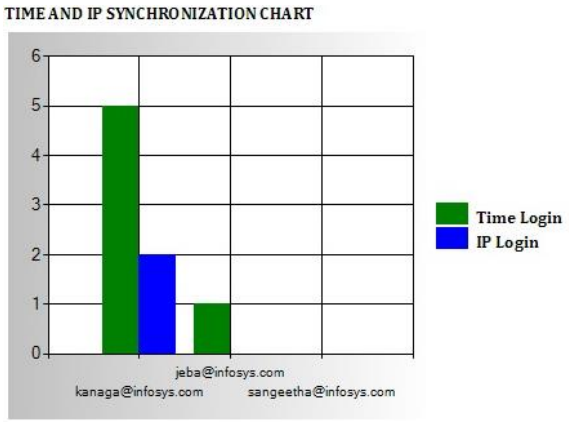

Fig 2. Time and IP overrule chart

Fig 1 show the user rights provided by the admin. Totally 2 users having compose rights, 3 users having inbox rights and 1 user having sent rights. This graph shows a clarity information about the rights. Fig 2. Shows the time and Ip trust wise. Here the Green chart denotes time exceed login users and Blue chart demotes IP exceed user details. User 1 login 5 times from non timing and 2 times from various IP adresss.

CONCLUSION

This project has been implemented successfully according to the committed abstract and all outputs have been verified. All the outputs are generating according to the given input. Data validations are done according to the user and admin input data. The employee's user name and password are generated in admin login, all the login has been verified successfully. Trust routing and aware routing

framework has been implemented successfully and result has been verified. Both routing frameworks are working according to the expected level. 'TaaS' working well for the 3 types of synchronization methods. And finally untrusted users can be find out easily using the above mention methods. So dual level security has been provided to the centralized server. Thus cloud armour has been implemented successfully and in efficient manner.

REFERENCE

[1] Trust Mechanisms for Cloud Computing. J. Huang and D.M.Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol.2,no.1,pp.1–14,2013

[2] Trusted Cloud Computing with Secure Resources and Data Colouring. K.Hwang and D.Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol.14, no.5,pp.14–22,2010.

[3] Towards a Trust Management System for Cloud Computing. S.Habib, S.Ries, and M.Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc.of TrustCom'11, 2011

[4] Service-oriented Computing and Cloud Computing: Challenges and Opportunities. Y .W ei and M.B.Blake, "Service-oriented Computing and Cloud Computing: Challenges and Opportunities," Internet Computing, IEEE, vol.14,no.6, pp.72–75,2010.

[5] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," Wireless Networks Journal (WINET), vol. 8, no. 5, pp. 521–534, Sep. 2002.

[6] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04). New York, NY, USA: ACM, 2004, pp. 59–64.

[7] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proceedings of the 7th international conference on Information processing in sensor networks (IPSN '08). IEEE Computer Society, 2008, pp. 245–256.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[21] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in Proceedings of Aerospace Conference, 2004.

[9] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefs-tathiou, C. Vangelatos, and L. Besson, "Design and implementa-tion of a trust-aware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3,Jul. 2010.

[10] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.

[11] S. Chang, S. Shieh, W. Lin, and C. Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS '06). New York, NY, USA: ACM, 2006, pp. 311–320.

[12] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sen. Netw., 2008.

[13] G. Zhan, W. Shi, and J. Deng, "Poster abstract: Sensortrust - a re-silient trust model for wsns," in Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (SenSys'09), 2009.

[14] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09). New York, NY, USA: ACM, 2009, pp. 1–14.