INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2116 - 2122
RECEIVED : 28-03-17. PUBLISHED: 22-04-17.

April 22, 2017

ENHNACED CLOUD SHIELD TRUST MANAGEMENT FOR CLOUD SERVICES

[1]Sowmiya.R, [2]Ashok Kumar.N,
[1]PG Scholar, Department of Computer Science and Engineering, Maharaja Engineering College, Coimbatore,
[2]Assistant Professor, Department of Computer Science and Engineering, Maharaja Engineering College, Coimbatore.

ABSTRACT

Here we are introducing a secured DNS with enhanced database which supports on cloud mail server. DNS is a relatively simple, text-based protocol, in which one or more recipients of a message are specified along with the message text and possibly other encoded objects performed in the absolute database. The message is then transferred to a remote server using a procedure of queries and responses between the client and server. Either an end-user's email client, MUA (Mail User Agent), or a relaying server's MTA (Mail Transport Agents) can act as an SMTP client in the server database. Here we introducing a procedure based security methodology called as instruction detection system (IDS) which trace the ip details, date, time and the password percentage of the hacker from the hacker's side. Hacker's location can be found out using their ip address. The details will be stored in the database from the server side. The DNS client initiates a TCP connection to server's port 25 (unless overridden by configuration). It is quite easy to test an SMTP server using the telnet program. DNS is a push protocol that does not allow one to pull messages from a remote server on demand. 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. It deals with preventing malicious parties and intrusion using trust aware routing framework with trust as a service. 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: DNS, SMTP, Database.

1. RELATED WORKS

Cloud computing refers to the underlying infrastructure for an emerging model of service provision that has the advantage of reducing cost by sharing computing and storage resources, combined with an on demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms.[1] Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. We begin this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations.[2]. Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data centre resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network

over multiple data centres to implement a reputation system for establishing trust between service providers and data owners.[3]. Cloud computing provides cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable, and shared services. Usually, cloud providers provide assurances by specifying technical and functional descriptions in Service Level Agreements (SLAs) for the services they offer [4]. Consumers' feedback is a good source to help assess overall trustworthiness of cloud services. However, it is not unusual that a trust management system experiences malicious behaviours from its users [5].

2. THE MODEL

ABOUT ROUTING PROCEDURE

This paper evaluates the proposed TARP protocols on two important attributes, the battery power and the software configuration. A secure route between a source and destination is established based on a confidence level prescribed by a user or application in terms of these attributes. Our performance evaluation shows that TARP is a robust and adaptive trust routing algorithm that reacts quickly and effectively to the dynamics of the network while still finding the shortest path to the destination. TARP is able to improve security and at the same time reduce the total routing traffic sent and received in the network by directing the traffic based on the requested sender attributes.

The Simple Mail Transfer Protocol (SMTP) service provided by IIS is a simple component for delivering outgoing e-mail messages. Delivery of a message is initiated by transferring the message to a designated SMTP server. Based on the domain name of the recipient e-mail address, the SMTP server initiates communications with a Domain Name System (DNS) server, which looks up and then returns the host name of the destination SMTP server for that domain.

Next, the originating SMTP server communicates with the destination SMTP server directly through Transmission Control Protocol/Internet Protocol (TCP/IP) on port 25. If the user name of the recipient e-mail address matches one of the authorized user accounts on the destination server, the original e-mail message is transferred to that server, waiting for the recipient to pick up the message through a client program.

SMTP is a delivery protocol only. It cannot pull messages from a remote server on demand. Other protocols, such as the Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP) are specifically designed for retrieving messages and managing mail boxes. However, SMTP has a feature to initiate mail queue processing on a remote server so that the requesting system may receive any messages destined for it (see Remote Message Queue Starting below). POP and IMAP are preferred protocols when a user's personal computer is only intermittently powered up, or Internet connectivity is only transient and hosts cannot receive message during off-line periods.

SMTP defines message transport, not the message content. Thus, it defines the mail envelope and its parameters, such as the envelope sender, but not the header or the body of the message itself. STD 10 and RFC 5321 define SMTP (the envelope), while STD 11 and RFC 5322 define the message (header and body), formally referred to as the Internet Message Format. Where a user is mobile, and may use different ISPs to connect to the internet, this kind of usage restriction is onerous, and altering the configured outbound email SMTP server address is impractical. It is highly desirable to be able to use email client configuration information that does not need to change.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2116 - 2122
RECEIVED : 28-03-17. PUBLISHED: 22-04-17.
April 22, 2017

3. ALGORITHM

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

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

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2116 - 2122
RECEIVED : 28-03-17. PUBLISHED: 22-04-17.
April 22, 2017

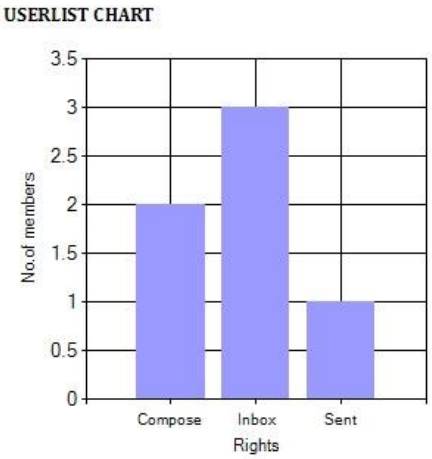
Return DTDiff

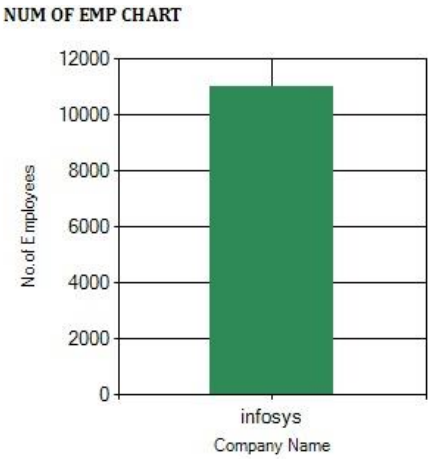
Suggest trust

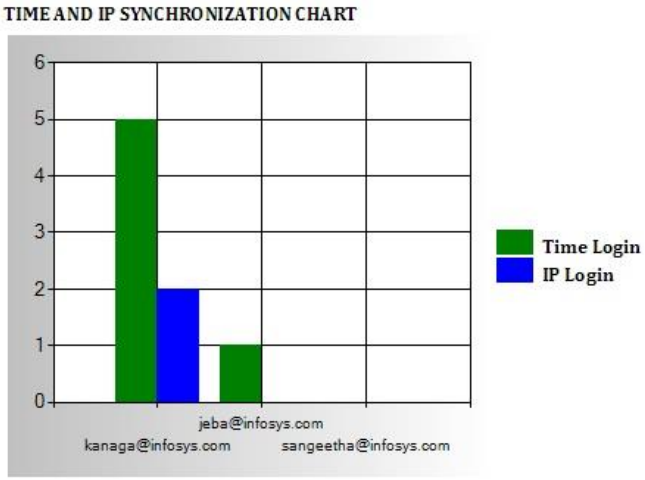
Stop Process

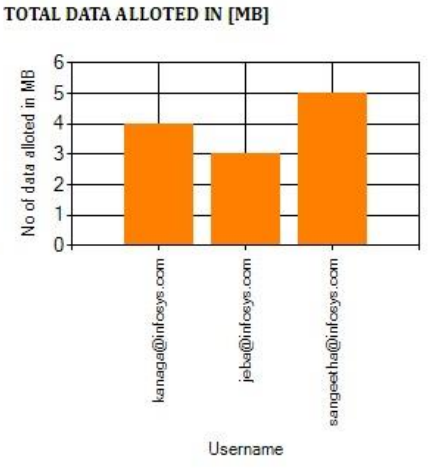
4. RESULT AND FINDINGS

This chapter deals with all the result and the obtain values from the available dataset. According to this paper, initially all the data will be considered as the input data and processing data. But as per proposed method we need to preprocess the data for a fine tuned result.









User List chart	Shows number of rights in the company
Num of Emp Chart	Shows number of employees in the company
Time and IP sych chart	Shows in dual chat with Time and IP sync details
Total Data Allotted	Number of data transferred from the company

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.

FUTURE WORK

Even thou the system has been developed in efficient manner, due to time constrain here by we gave some provisions for future enhancements. All the database design is created according to the future work. And all provisions are made in this application according to the future enhancement. The best suit for future work in Green Computing; this is because, now the architecture is developed in cloud environment and it performing well. The next to cloud architecture is green computing which makes the system more powerful and efficient.

Mobile Responsive: In future this application can be made as mobile responsive application. This makes the admin to handle all the features in a single mobile device or in a tablet.

Enhance Security: Security can be improved by adding, superior security methods like biometric or Voice security for admin. This makes the admin zone more secured.

Data ware house: Storage server can be improved; the current and existing projects can be stored in the centralized server. This makes the developer to refer with the existing code for code reusability methods.

Offline Architecture : In case of non availability of internet, all these options can be operated in internal LAN architecture. All the data transfer can be made in offline also.

Performance : In case if implementing this application in green computing architecture, the performance can be improved. This makes more data transaction at a same time.

REFERENCE

[1] A. Wood and J. Stankovic, "Denial of service in sensor networks,"Computer, vol. 35, no. 10, pp. 54–62, Oct 2002.

[2] M. Jain and H. Kandwal, "A survey on complex wormhole attackin wireless ad hoc networks," in Proceedings of International Con-ference on Advances in Computing, Control, and Telecommunication Technologies (ACT '09), 28-29 2009, pp. 555 –558.

[3] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sink-hole attack in wireless sensor networks; the intruder side," in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB '08), 12-14 2008, pp. 526 –531.

[4] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analy-sis of mobile agent-based wireless sensor network," in Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 –19.

[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.

[15] G. Zhan, W. Shi, and J. Deng, "Design, implementation and evaluation of tarf: A trust-aware routing framework for dynamic wsns," http://mine.cs.wayne.edu/guoxing/tarf.pdf, Wayne State University, Tech. Rep. MISTTR2010-003, Oct. 2010.