ENHANCED WEB ARCHITECTURE FOR MAIL PRIVACY AND PRESERVATION USING CLOUD COMPUTING

[1]P.V.Kavitha, [2]G.S.Akshaya, [3]T.Kirthana, [4]U.Monisha
[1]Assistant Professor (Sr.G), Department of Information Technology,
Sri Ramakrishna Engineering College,
[2,3,4]UG Scholar,Department of Information Technology,
Sri Ramakrishna Engineering College.

ABSTRACT

The anchored DNS with upgraded database which underpins on cloud mail server. DNS is a generally straightforward, content based convention, in which at least one beneficiaries of a message are indicated alongside the message content and perhaps other encoded objects performed in the outright database. The message is then exchanged to a remote server utilizing a method of questions and reactions between the customer and server. Either an end-client's email customer, MUA (Mail User Agent), or a transferring server's MTA (Mail Transport Agents) can go about as a SMTP customer in the server database. Here we presenting a technique based security strategy called as intrusion Detection system (IDS) which follow the IP subtleties, date, time and the secret phrase level of the programmer from the programmer's side. Programmer's area can be discovered utilizing their IP address. The subtleties will be put away in the database from the server side. The DNS customer starts a TCP association with server's port 25 (except if superseded by setup). It is very simple to test a SMTP server utilizing the telnet program. DNS is a push convention that does not enable one to pull messages from a remote server on interest. With the goal that the primary article is to make security conservation for the classified database the proposed design executes this present reality mysterious database by actualizing the speculation and concealment. It manages anticipating vindictive gatherings and interruption utilizing trust mindful steering system with trust as an administration. The proficiency and security of information can be accomplished by keeping up single database with explicit access rights. With the activity performed with IDS with ESMTP in Anonymous and Confidential Databases.

Keywords: Enhanced SMTP, Intrusion Detection system, DNS, mail Exchange.

RELATED WORKS

Distributed computing alludes to the fundamental framework for a developing model of administration arrangement that has the benefit of decreasing expense by sharing figuring and capacity assets, joined with an on interest provisioning component depending on a compensation for each utilization plan of action. These new highlights directly affect data innovation (IT) planning yet in addition influence conventional security, trust and protection mechanisms.[1] Trust is a basic factor in distributed computing; in present practice it depends to a great extent on view of notoriety, and self evaluation by suppliers of cloud administrations. We start this paper with an overview of existing instruments for building up trust, and remark on their limitations.[2]. Trust and security have kept organizations from completely tolerating cloud stages. To ensure mists, suppliers should initially anchor virtualized server farm assets, maintain client security, and save information trustworthiness. The creators recommend utilizing a trust-overlay organize over various server farms to execute a notoriety framework for building up trust between specialist organizations and information owners.[3]. Distributed computing gives cost-productive chances to endeavors by

offering an assortment of dynamic, adaptable, and shared administrations. For the most part, cloud suppliers give affirmations by determining specialized and practical depictions in Service Level Agreements (SLAs) for the administrations they offer [4]. Buyers' input is a decent source to help survey by and large reliability of cloud administrations. Be that as it may, it isn't irregular that a trust the executives framework encounters malevolent practices from its clients [5].

INTRODUCTION

The communication across the world is must in the modern age communications through postal may take more time. It may be days or weeks to make the message available to others.

E-Mail service details with the web site that manage the electronic way of communication. Through this thesis we can create our own user id, sends mails to any user and manage inbox. In addition greetings can be send to friends. We can view incoming mails and greetings and even delete them. Resume can be stored and changed whenever necessary. Any mail related report can be viewed through the site. Deletion of unwanted mails can be made to manage memory. This is one of the problem in the existing system is said as detecting denial of service attacks.

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. 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 provided. MUA (Mail User Agent), or a relaying server's MTA (Mail Transport Agents) can act as an SMTP client. This design can also can be implemented in wireless sensor networks.

An email client knows the outgoing mail SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the email address to the right of the **at** (**@**) sign). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. Some current mail transfer agents will also use SRV records, a more general form of MX, though these are not widely adopted. (Relaying servers can also be configured to use a smart host.)

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.

There are two main components available in this thesis trust and aware routing, So that according to the procedure trust is implemented for user rights, in order to provide a user authentication mode. These authentication modes are in the customized format in order to provide rights to the appropriate users from the admin side. In added with aware routing is working under the principle of IDS (Instruction detection system) which detects the third part authorization, hackers, attackers and data privacy with their corresponding IP address with their date and time.

PRIMARY OBJECTIVE

The main objective of this project is to develop a trust aware routing environment using SMTP server. Here an email environment is developed for a organization, trust is implemented for user rights as well as aware routing is implemented for security purpose. For special security purpose here we introducing a latest method called as IDS (Instruction detection system), which identified the third party intruder or hacker from other networks. The basic IDS can able capture the ip details, here we using a advanced IDS method which can able to capture ip address of the hacker, data, time and the password which he tries to hack. In added with the trust method will provide the user rights within the organization.

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.z

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.

ALGORITHM

INITIALIZATION:

IP – Internet protocol synchronization
DT - Date synchronization
TM – Time Synchronization
M – Mail
TR – Trust

ALGORITHM PROCESS

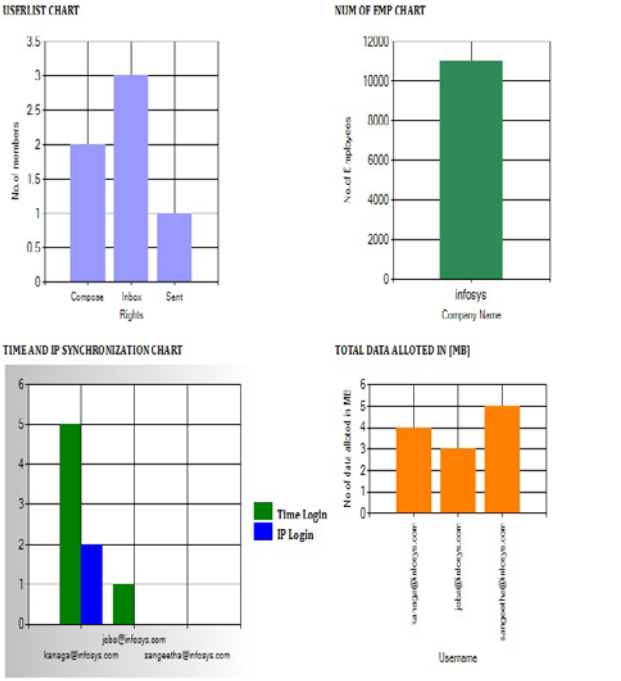
Start Process
User login from SMTP
DateTimeDateTimeDiff (Mail M)
Get system date/time in SysDT
if (Received Filed is present in M) do

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 SysDTandRecentResDT 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

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 executed effectively as mentioned by the commited abstract and the sum total of what yields have been confirmed. Every one of the yields are creating as per the given info. Information approvals are finished by the client and administrator input information. The representative's client name and secret word are produced in administrator login, all the login has been confirmed effectively. Trust directing and mindful steering system has been actualized effectively and result has been confirmed. Both directing systems are working as indicated by the normal dimension. 'TaaS' functioning admirably for the 3 sorts of synchronization strategies. Lastly untrusted clients can be discover effectively utilizing the above notice strategies. So double dimension security has been given to the concentrated server. Along these lines cloud covering has been executed effectively and in productive way.

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.

REFERENCES

[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 Conference 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.