Enhanced Cloud Armor: Using Privacy and Preservation Framework for ESMTP Server

[1]A Muthuraja Boopathy, [2]B. Naveen kumar, [3]R. Udhayakumar and [4]P. Kalpana

[1, 2, 3] Student, Dept. of CSE, Sri Krishna College of Technology, Coimbatore.

[4] Assistant Professor, Dept. of CSE, Sri Krishna College of Technology, Coimbatore.

ABSTRACT

The main objective of the project is to develop a trust aware routing environment using SMTP server. An email environment is developed for an organization, trust is implemented for user rights as well as aware routing is implemented for security purpose. For special security purpose 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 to capture the IP details, using an 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. It deals with preventing malicious parties and intrusion using trust aware routing framework. The efficiency and security of data can be achieved by maintaining single database with specific access rights. Trust management is one of the most challenging issues for the adoption and growth of cloud computing. There are several challenging issues in the trust management such as privacy, security, and availability. These process threatening the entire cloud users. This is because cloud can be access anywhere at any time. The disadvantage levels are equal to the advantage level. 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

KEYWORD: Trust Routing Framework, Aware, Routing Framework.

1. INTRODUCTION

The main objective is to develop a trust aware routing environment using SMTP server. Here an email environment is developed for an 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 an 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

1.2 THE ARCHITECTURE MODEL

E-mail communication is indispensable nowadays but the e-mail spam problem continues growing drastically. In recent years, the notion of collaborative spam filtering with near-duplicate similarity matching scheme has been widely discussed. The primary idea of the similarity matching scheme for spam detection is to maintain a known spam database, formed by user feedback, to block subsequent near-duplicate

spams. On purpose of achieving efficient similarity matching and reducing storage utilization, prior works mainly represent each e-mail by a succinct abstraction derived from e-mail content text. However, these abstractions of e-mails cannot fully catch the evolving nature of spasm, and are thus not effective enough in near-duplicate detection. In this paper, we propose a novel e-mail abstraction scheme, which considers e-mail layout structure to represent e-mails. We present a procedure to generate the e-mail abstraction using HTML content in e-mail, and this newly devised abstraction can more effectively capture the near-duplicate phenomenon of spasm. Moreover, we design a complete spam detection system Codes (standing for Collaborative Spam Detection System), which possesses an efficient near-duplicate matching scheme and a progressive update scheme. The progressive update scheme enables system Codes to keep the most up-to-date information for near-duplicate detection. We evaluate Codes on a live data set collected from a real e-mail server and show that our system outperforms the prior approaches in detection results and is applicable to the real world.

1.3 MESSAGE ARCHITECTURE

E-MAIL SERVER consists of core modules

1. Separating mails
2. Deduction of spam mails
3. Sorting mails
4. Hacker list
5. IP Address tracker

2. LITERATURE SURVEY

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)[4] budgeting but also affect traditional security, trust and privacy mechanisms. The advantages of cloud computing its ability to scale rapidly, store data remotely and share services in a dynamic environment can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. Some core traditional mechanisms for addressing privacy (such as model contracts) are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm[8]. In this chapter we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed. Although there is no definitive definition for cloud computing, a definition that is commonly accepted is provided by the United States National Institute of Standards and Technologies (NIST): This shared pool of resources is unified through virtualisation or job scheduling techniques. Virtualisation is the creation of a set of logical resources (whether it be a hardware platform, operating system, network resource or other resource)[9] usually implemented by software components that act like physical resources. In particular physical computer hardware and thus allows the operating system software running on the virtual platform a virtual machine (VM) to be separated from the underlying hardware resources. The resources made available through cloud computing include hardware and systems software on remote data centres as well as services based upon these that are accessed through the Internet these resources can be

managed to dynamically scale up to match the load, using a pay-per resources business model[3]. Key features advertised are elasticity, multi tenancy, maximal resource utilization and pay-per-use. These new features provide the means to leverage large infrastructures like data centres through virtualization or job management and resource management.[1] Cloud computing (or, more with a huge potential both for efficiency and new business opportunities (especially in service composition) and is almost certain to deeply transform our information technology infrastructures, models and services. Not only are there cost savings due to economies of scale on the service provider side and pay-as-you-go models but business risk is decreased because there is less need to borrow money for upfront investment in infrastructure The adoption of cloud computing may move quite quickly depending on local requirements, business context and market specificities. Still in the early stages but cloud technologies are becoming adopted widely in all parts of the world.

The economic potential of cloud computing and its capacity to accelerate innovation are putting business and governments under increased pressure to adopt cloud computing based solutions [6]. Although the hype around cloud tends to encourage people to think that it is a universal panacea this is not the case and quite often promoters ignore the inherent complexities added by the cloud. There are a number of challenges to providing cloud computing services the need to comply with local and regional regulations, obtaining the necessary approvals when data is accessed from another jurisdiction, some additional complexity in terms of governance, maintenance and liability inherent to cloud, and a perceived lack of trust in cloud services.

Cloud computing has become a prominent paradigm of computing and IT service delivery. The context of cloud computing. What is the basis of that trust? If the attributes of a cloud service (or a service provider) are used as evidence for trust judgment on the service (or provider respectively), on what basis should users believe the attributes claimed by cloud providers? Who are authorities to monitor, measure, assess, or validate cloud attributes? The answers to those questions are essential for wide adoption of cloud computing and for cloud computing to evolve into a trustworthy growing importance of cloud computing makes it increasingly imperative that we grapple with the meaning of trust in the cloud and how the customer, provider, and society in general establish cloud computing have been widely discussed from different perspectives. A number of models and tools have been proposed. Each contributes a partial view of cloud trust, but lacking still is a complete picture illustrating how cloud entities solid grounding in trust, serving to facilitate trusted paths to trusted cloud services.

The NIST Cloud Computing Reference Architecture identified cloud brokers and cloud auditors as entities who conduct assessment of cloud services[2] however, there are few studies on trust relation analysis and the chains of trust from cloud users to cloud services (or providers) through those intermediary cloud entities. In this paper, we investigate trust mechanisms for the cloud, present our vision of the framework for analyzing trust relations in the cloud, and suggest trust mechanisms which combine

attribute certification, evidence-based trust and policy-based trust.

Because of the criticality of many computing services and tasks, some cloud clients cannot make decisions about employing a cloud service based solely on informal trust mechanisms (e.g. web-based reputation scores); these decisions need to be based on formal trust mechanisms, which are more certain, more accountable, and society. In our suggested cloud trust mechanisms, the attributes of a cloud service (or its provider) are used as evidence of the service (or provider), and the belief in those chains of trust for validation focus somewhat informally on the conceptual basis for analysis of trust in the cloud we do not at this time address mathematical modelling which would involve many more precise details, formal languages and specific use cases.

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. Data colouring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds.

3. DESIGN METHODOLOGY

3.1 PROBLEM STATEMENT

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service)is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of Cloud Armor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes

i) A novel protocol to prove the credibility of trust feedbacks an privacy,

ii) An adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and

iii) An availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feed backs on cloud services.

3.2 PROPOSED SYSTEM: - ENHANCEMENT

Techniques Used:

ESMTP Enhanced Simple Mail Transfer Trust as a Service User Rights Aware as a Service IDS (Intrusion Detection System) IP Synchronization Algorithm: C4.5- STATISTICAL CLASSIFIER

All the drawback in the existing has been over came in the proposed system. In the proposed system an organization environment has been used for implementing both trust and aware framework. Here SMTP server has been enhanced as ESMTP for implement Trust as a service and IDS has been implemented for Aware as a service. The Enhanced Simple Mail Transfer Protocol (ESMTP) service provided by IIS(Internet Information Service) is a component for delivering outgoing e-mail messages for a DNS(Domain Name server) based SMTP. Delivery of a message is initiated by transferring the message to a designated ESMTP 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. The originating SMTP server communicates with the destination SMTP server directly through Transmission Control Protocol/Internet Protocol (TCP/IP) on port 25. Each port can make up to 1 lakh communication.

The ESMTP is a flexible mail server which can be implemented in various environments like IT Organizations, Private Organization, Government sectors and etc. And ESTMP can be customized more up to the user favor. This protocol supports multiple file types, various security levels, multiple organization and etc. All these techniques come under a single architecture. As per existing the cloud armor deals with customer feedback in a public cloud. According to the activity of the users, the trustworthiness of the user or customer will be evaluated. Here the trust as a service has been modified according to trust routing framework. The ESMTP has been customized according to the admin procedure. So that admin can provide user rights to the employee by customizing the mail components like compose, inbox, send items and etc. The customized mail server will reflect to the users login and mail will response for unidirectional. For Aware routing framework, intrusion detection has been implemented. The IDS will capture all the Password used, Password matching percentage and times of hacking. This makes the admin more from the intruder and hacker side. And finally the color code has been implemented for secured login. For color code quantum cryptography has been used. A color grid is available with various colors. User can select any three colors for secured login. In added with Gaussian mixture and keystroke has been implemented for pattern based password login.

Advantages of the proposed system

1. A private mail server will be created for the company, So that from the mail server each user will be provided with the individual DNS.
2. More trust has been implemented.
3. A Prior user rights will be provided for the users. This control will be made by the admin.

4. Admin can customize the mail component of the users like compose, inbox, outbox, send items and etc.
5. In case of change of password by the user, a notification will be sent to the admin. So that admin can able to view the changed username and password.
6. Intruder will be identified using instruction detection technique.
7. In date, time, password used and ip address of the hacker will be recorded in the data grid.
8. The intruder detection method will be applicable for both admin and user.

4. DESIGN METHODOLOGY

4.1 APPLICATION SPECIFICATION

CLIENT/SERVER ARCHITECTURE:

Benefits offered by client/server architecture:

- Increased user communication because of flexible data access.
- Highly interactive user interface.
- Increased developer productivity through usage of easy to use easy tools.
- Improved access to information because of networking.
- Better control of corporate data through centralized data, systems & network management.
- Easier maintenance of application & data. Protection of hardware investments by making use of existing installations of Hardware, software & network and at same time getting maximum leverage out of the available desktop technology.

4.2 NETWORK SPECIFICATION

(i) Windows 7 Platform

Windows 7 is a powerful multitasking operating system with high security. It is user friendly and supports multithreading and lot of tools for developing any application. This OS has number of enhancements, including performance improvements, better hardware support and closer integration with the Net. Windows support dynamic linking. This OS has the concept of plug and play.

(ii) IIS -Application Server

IIS is the Internet Information Server. The thesis is a web- based thesis. It needs an application server to run. IIS is an application server where the thesis runs. This application server is chosen because the thesis is developed in ASP and both of them are Microsoft products. Performance will be good if the product is form the same company. IIS is user-friendlier than other application servers. Some of its features are,

1. High performance network and application server.
2. The server includes the Secure Sockets Layer (SSL) encrypted communication standard for private communication between the clients and server.
3. Active Server page allows application with scripts and components to perform multiple actions.
4. With Windows NT service pack. It also acts as a web server.

(iii) Personal Web Server

Personal Web Server (PWS) is the server designed for developing sites offline. It supports many of the features seen in the full

version of IIS including virtual directories and Active Server Pages. Server administration is straightforward and simple-much like administration of its larger counterpart. IIS administration, which is dialog-based while PWS administration is web based. Personal Web Server properties dialog box reveals the two services: HTTP and FTP. It does not provide the Gopher service available in IIS.

4.3 ABOUT SMTP

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.

In the case where the originating SMTP server cannot communicate directly with the destination server, the SMTP service can transfer messages through one or more intermediate relay SMTP servers. A relay server receives the original message and then delivers it to the destination server, or redirects it to another relay server. This process is repeated until the message is delivered or a designated timeout period passes.

The SMTP service is not installed by default. You must install the SMTP service using the Control Panel. Installing the SMTP service creates a default SMTP configuration which you can then customize to your needs using IIS Manager.

4.4 SMTP Vs Mail retrieval

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. Remote Message Queue Starting is a feature of SMTP that permits a remote host to start processing of the mail queue on a server so it may receive messages destined to it by sending the TURN command. This feature however was deemed insecure[15] and was extended in RFC 1985 with the ETRN command which operates more securely using an authentication method based on Domain Name System information.

5. SMTP INTERFACE MODEL

5.1 Outgoing mail SMTP server

An e-mail client needs to know the IP address of an SMTP server and this has to be given as part of its configuration (usually given as a

DNS name). The server will deliver outgoing messages on behalf of the user.

5.2 Outgoing mail server access restrictions

Server administrators need to impose some control on which clients can use the server. This enables them to deal with abuse, for example spam. Two solutions have been in common use. In the past, many systems imposed usage restrictions by the location of the client, only permitting usage by clients whose IP address is one that the server administrators control. Usage from any other client IP address is disallowed. Modern SMTP servers typically offer an alternative system that requires authentication of clients by credentials before allowing access.

5.3 Restricting access by location

Under this system, an ISP's SMTP server will not allow access by users who are 'outside the ISP's network'. More precisely, the server may only allow access to users with an IP address provided by the ISP, which is equivalent to requiring that they are connected to the Internet using that same ISP. A mobile user may often be on a network other than that of their normal ISP, and will then find that sending email fails because the configured SMTP server choice is no longer accessible.

This system has several variations. For example, an organization’s SMTP server may only provide service to users on the same network, enforcing this by firewalling to block access by users on the wider Internet. Or the server may perform range checks on the client's IP address. These methods were typically used by corporations and institutions such as universities which provided an SMTP server for outbound mail only for use internally within the organization. However, most of these bodies now use client authentication methods, as described below.

By restricting access to certain IP addresses, server administrators can readily recognise the IP address of any abuser. As it will be a meaningful address to them, the administrators can deal with the rogue machine or user.

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.

5.4 Client authentication

Modern SMTP servers typically require authentication of clients by credentials before allowing access, rather than restricting access by location as described earlier. This more flexible system is friendly to mobile users and allows them to have a fixed choice of configured outbound SMTP server.

5.5 MAIL PROCESSING MODEL

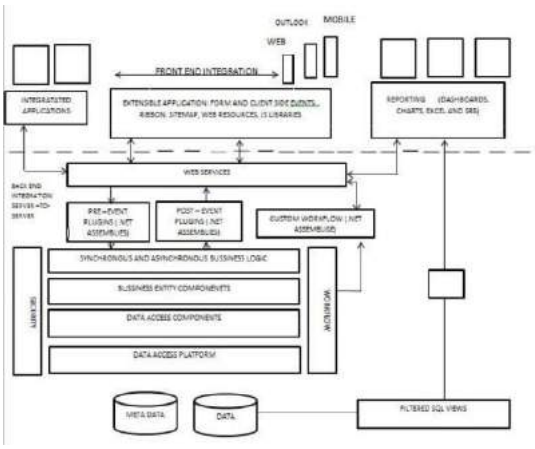
Email is submitted by a mail client (MUA, mail user agent) to a mail server (MSA, mail submission agent) using SMTP on TCP port 587. Most mailbox providers still allow submission on traditional port 25. From there, the MSA delivers the mail to its mail transfer agent (MTA, mail transfer agent). Often, these two agents are just different instances of the same software launched with different options on the same machine. Local processing can be done either on a single machine or split among various appliances in the former case involved processes can share files in the latter case, SMTP is used to transfer the message internally with each host configured to use the next appliance as a smart

host. Each process is an MTA in its own right that an SMTP server.

The boundary MTA has to locate the target host. It uses the Domain name system (DNS) to look up the mail exchanger record (MX record) for the recipient's domain. The returned MX record contains the name of the target host. The MTA next connects to the exchange server as an SMTP client. (The article on MX record discusses many factors in determining which server the sending MTA connects to.)

Once the MX target accepts the incoming message, it hands it to a mail delivery agent (MDA) for local mail delivery. An MDA is able to save messages in the relevant mailbox format. Again, mail reception can be done using many computers or just one the picture displays two nearby boxes in either case. An MDA may deliver messages directly to storage, or forward them over a network using SMTP, or any other means, including the Local Mail Transfer Protocol (LMTP), a derivative of SMTP designed for this purpose. Once delivered to the local mail server, the mail is stored for batch retrieval by authenticated mail clients (MUAs). From fig 5.5.1.Mail is retrieved by end-user applications, called email clients, using Internet Message Access Protocol (IMAP), a protocol that both facilitates access to mail and manages stored mail, or the Post Office Protocol (POP) which typically uses the traditional mbox mail file format or a proprietary system such as Microsoft Exchange/Outlook or Lotus Notes Domino. Webmail clients may use either method, but the retrieval protocol is often not a formal standard.

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.



5.5.1. MAIL PROCESSING FLOW DIAGRAM

7. CONCLUSION AND FUTURE SCOPE

Given the highly dynamic, distributed, and nontransparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. Cloud service users feedback is a good source to assess the overall trustworthiness of cloud services. However malicious users may collaborate together to disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or trick users into trusting cloud services that are not trustworthy by creating accounts and giving misleading trust . In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time. We also develop an availability model that maintains the trust management service at a desired level. The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors. There are a few directions for our

future work. We plan to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future.

REFFERENCE

[1] CloudArmor: Supporting Reputation-based Trust Management for Cloud Services Talal H. Noor, Quan Z. Sheng, Member, IEEE, LinaYao, Member, IEEE, Schahram Dustdar, Senior Member, IEEE, and Anne H.H. Ngu, IEEE TRANSACTIONS ON PARALL EL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 2, FEBRUARY 2016.

[2] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefs-tathiou, C. Vangelatos, and L. - tion of a trust- International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3,Jul. 2010

[3] complex wormhole attackin wireless ad hoc - ference on Advances in Computing, Control, and Telecommunicat), 28-9-2009, pp. 555 558.

[4] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, -sis of mobile agent-based International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 19.

[5] library for elliptic curve cryptography in wireless international conference on Information processing EE Computer Society, 2008, pp. 245 256.

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, -hole attack in wireless sensor IEEE International Conference on Wireless and Mobile Computing, Networking and -14 2008, pp. 526 531.

[7]-aware routing protocol for sensor-actuator Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.

[8] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Proceedings of the 2nd ACM workshop on Security York, NY, USA: ACM, 2004, pp. 59 64.

[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, IEEE Communications Magazine, vol. 40, no. 8, pp. 102 114, Aug. 2002.

[10] A. Perrig, R. Szewczyk, W. Wen, D. Culler, protocols for sensor vol. 8, no. 5, pp. 521