ADVANCED MAIL SERVER USING FIRE EYE DETECTION SYSTEM

[1]Mouthami K, [2]Divyabharathi S, [3]Jayashree M, [4]Nandita S, [5]Shalini M

[1]M.E, Phd, Assistant Professor, Department of Information Technology-Dr.N.G.P IT-Coimbatore-India,
[2]BTech Scholar-Department of Information Technology-Dr.N.G.P IT-Coimbatore-India,
[3]BTech Scholar-Department of Information Technology-Dr.N.G.P IT-Coimbatore-India,
[4]BTech Scholar-Department of Information Technology-Dr.N.G.P IT-Coimbatore-India,
[5]BTech Scholar-Department of Information Technology -Dr.N.G.P IT-Coimbatore-India.

Abstract :

Trust management is one of the significant issues in the Information Technology for the selection and development of IT Companies. The serious issue looking altogether IT organizations during work from home are hacking and information abuse, through hacking a mail server, the organization's whole innovation can be taken from the fundamental mail server. This is on the grounds that Mail Server can be gotten to anyplace. Through this venture we can make our own cloud mail worker with ESMTP – Enhanced Simple Mail Transfer Protocol. To conquer these issues in this task we presenting a got mail Server with improved data set which upholds on various secured mail server. Here we presenting a technique based security approach called as Fire Eye Detection System (FEDS) which follows the IP details, date, time and the secret phrase level of the programmer from the programmer's side. SMTP worker can be effortlessly tried utilizing the telnet program. DNS doesn't permit one to pull messages from a distant worker on request since it follows push convention. Thus, the fundamental target is to make protection safeguarding for the secret data set. The proposed engineering executes this present reality mysterious data set by carrying out the speculation and concealment during telecommute. With the activity performed with FEDS and ESMTP in Anonymous and Confidential Databases with explicit access rights we can accomplish the effectiveness and security of information.

Keywordss - FEDS; ESMTP; Trust aware routing framework; IP synchronization; Trust-as-a-service (Taas).

I. INTRODUCTION

The thesis named "ADVANCED MAIL SERVER USING FIRE EYE DETECTION SYSTEM" is planned utilizing Active Server Pages .NET with Microsoft Visual Studio.Net 2012 as front end and Microsoft SQL Server 2010 as back end which works in .Net system variant 2.0. The coding language utilized is ASP.Net. The communication across the world is must in the advanced age interchanges through postal may take additional time. It might be days or weeks to make the message accessible to other people. Email administration subtleties with the site that deal with the electronic method of correspondence. Through this proposition we can make our own client id, sends to any client and oversee inbox. Moreover good tidings can be ship off companions. We can see approaching sends and good tidings and even erase them. Resume can be put away and changed at whatever point important. Erasure of undesirable sends can be made to oversee memory. This is one of the issue in the current framework is said as distinguishing disavowal of administration assaults.

II. LITERATURE SURVEY

Portable specialist framework gives us another approach to acknowledge appropriated synergistic data preparing in sensor organizations. In this paper, we present a middleware to acknowledge versatile specialist put together information combination with respect to remote sensor networks hubs, which is carried out totally in TinyOS and has been tried on TelosB bits. It comprises of two sections. One is the technique for the serialization of calculation in portable specialists in type of character string. The other is a mediator written in nesC language which is utilized to decipher and deserialize the customized calculation character string to orders, and execute orders line by line. We present TinySec, the trust completely carried out interface layer security engineering for remote sensor organizations. In our plan, we influence ongoing exercises gained from plan weaknesses in security conventions for other remote organizations like 802.11b and GSM. With little recollections, feeble processors, restricted energy, and 30 byte bundles, sensor networks can't bear the cost of this extravagance. Our exploratory outcomes on a 36 hub disseminated sensor network application plainly exhibit that product based connection layer conventions are doable and proficient, adding under 10% energy, inertness, and transmission capacity overhead. Steering conventions are the limiting power in versatile specially appointed organization since they work with correspondence past the remote transmission scope of the hubs. Be that as it may, the foundation less, inescapable, and dispersed nature of MANETs renders them helpless against security dangers. In this paper, we propose a novel group based trust-mindful directing convention for MANETs to shield sent parcels from go-between malevolent hubs. The proposed convention puts together the organization into one-bounce disjoint bunches at that point chooses the top and dependable hubs for assume the part of group heads that are liable for taking care of all the directing exercises. The Trust-installed AODV (T-AODV) steering convention was planned by us to get the specially appointed organization from autonomous malignant hubs by tracking down a safe start to finish course. In This work we have proposed an expansion of T-AODV that can withstand assault by different malevolent hubs acting in arrangement to upset the organization. In this regard, the arrangement is novel and, apparently, the principal such arrangement proposed up until now. We have shown the productivity of our convention by broad re-enactment and furthermore broke down its security by assessing diverse danger situations.

III. PROPOSED SYSTEM

Advanced DNS /POP3 Email Server has tons of features like mailing lists, anti-spam, multiple DNS gateways, security and compatibility with any email program. It can be used as a dedicated mail server, or as a personal local SMTP server. The DNS relay server allows relay emails sent directly to their destination, by passing through provider's mail server. Without the help of your ISP, DNS server program sends email messages, directly from your local PC to recipient mailboxes and can choose your favorite email client with this software which you used to do it before. DNS relay software allows emails directly to receiver mailbox. This is much faster and reliable than using DNS server provided by your ISP. Powerful direct remailer software act as DNS relay. 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. A user rights will be provided for the users which will be controlled by the admin. The mail component of the users like compose, inbox, outbox, send items and etc can be customized by the admin. While password is changed by the user, a notification will be sent to the admin. The changed username and password can be view by the admin. When the intruder tries to attack, the user's hacking date, time, password used and IP address of the hacker will be recorded in the data grid. Using intrusion detection technique both admin and user can identify the intruder. All emails can read and saved by using only the key.

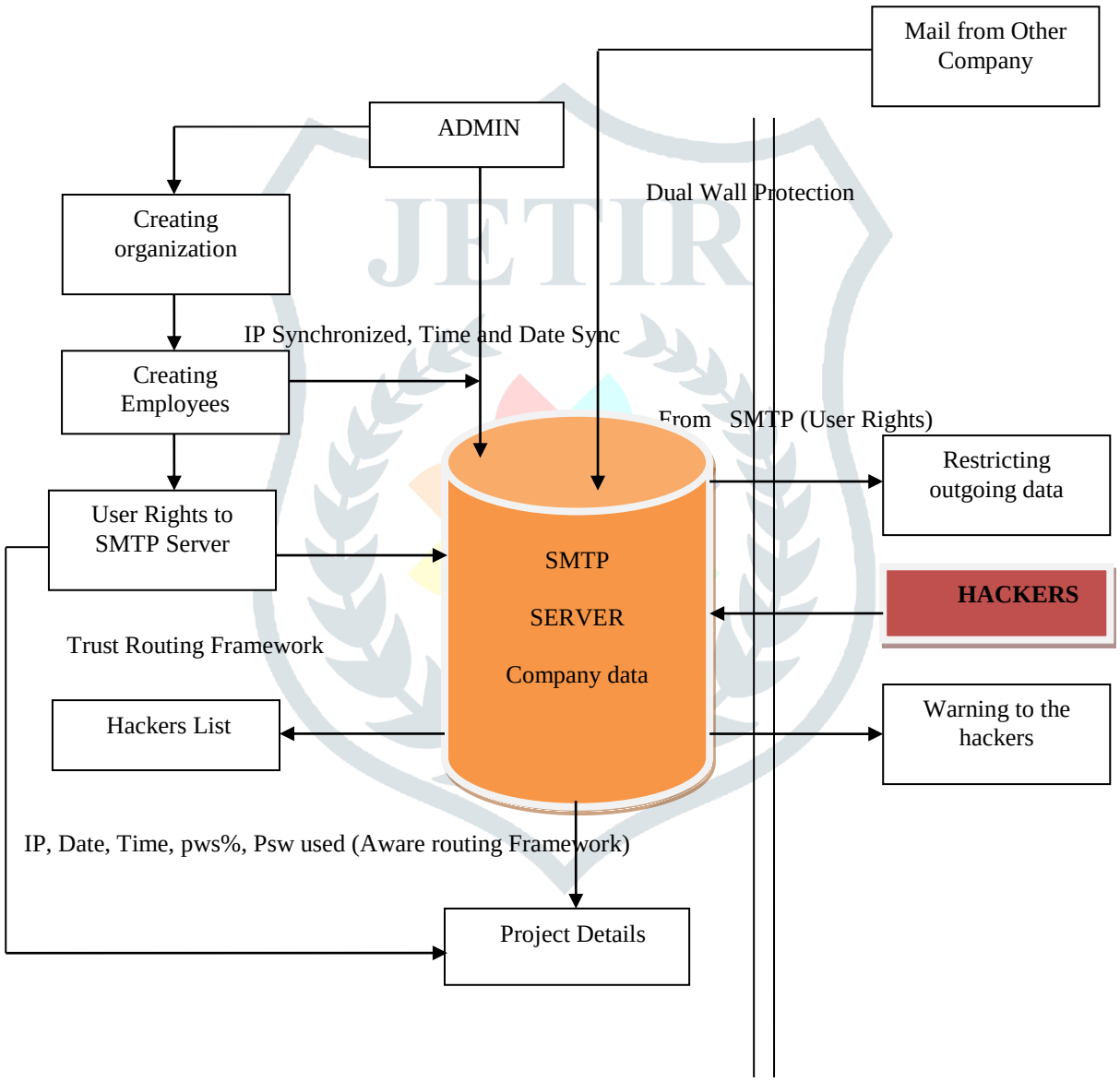

Fig.1 Proposed System Architecture

IV. SYSTEM ARCHITECTURE

4.1 Routing Procedure

Security could be an important issue during a mobile ad hoc network. In most of the previous protocols, security is a new layer on top of the routing protocol. We tend to propose a Trust Aware Routing Protocol for secure-trusted routing in mobile ad hoc networks. In TARP, security is inherently designed into the routing protocol where each node evaluates the trust level of its neighbors supported a gaggle of attributes and determines the route supported these attributes. This paper evaluates the planned tarp protocols on 2 vital attributes, battery power and also computer code configuration. A secure route between a supply and destination is established supported by a confidence level prescribed by a user or application in terms of those attributes. Our performance analysis shows that canvas could be a sturdy and accommodative trust routing rule that reacts quickly and effectively to the dynamics of the network whereas still finding the shortest path to the destination. Canvas is in a position to

enhance security and at a similar time cut back the entire routing traffic sent and received within the network by leading the traffic supported by the requested sender attributes.

4.2 Trust Aware Routing Protocol

TARP selects routes to the destination primarily based not only on the shortest path however additionally on much different security adjusted attributes of the nodes. Only nodes that match the sender necessities would forward the packet. The main objectives of the planned TARP suite are:

i. Implement security that's inherently engineered into the routing protocol,
ii. Deliver messages that square measure received with a user-outlined or best obtainable level of confidence,
iii. Enable users and applications to inflict their needed level of security,
iv. Deliver the potency of the good in routing that's improved by limiting management message exchanges, optimize resource usage,
v. Get switch network performance degradation, and develop a protocol suite that adapts to changes within the surroundings, like the topology, the power-level of nodes, etc.

In TARP, the protection parameters thought about in computing the trust-level of a node in an exceedingly given route include package configuration, hardware configuration, battery power, credit history, exposure, and structure hierarchy. Every node evaluates the trust level of its neighbors supported on top of parameters and includes it in computing consecutive hop nodes within the overall shortest route computation. This paper can target the implementation and analysis of the battery power and therefore the package configuration attributes. Below may be a description of the battery power and package configuration attributes:

• Power: In wireless networks, the battery power with that node operate may be a restricted resource. Every node uses its power to not solely send and receive, it conjointly behaves as a router by forwarding routing messages and updates. The cryptological techniques that give security square measure computationally intensive, that any increase the ability consumption of a node. The node's trust level ought to be set to low since it cannot guarantee its service. This illustrates that power is a vital parameter for evaluating the trust level of a node.

• Package Configuration: The package configuration includes the encoding ability of a node. To satisfy CAI ,completely different cryptological mechanisms are planned. Some square measures supported symmetrical encoding et al on uneven encoding. Every node is given either a shared secret key or a public/private key combine betting on the sort of cryptological mechanism. Completely different encoding algorithms square measure obtainable like RSA, DES/3DES, BLOWFISH, IDEA, SEAL RC2/RC4/RC5/RC6 [12]. Robust encoding is usually discerned by the key length utilized by the algorithmic rule. In general, a node with a stronger encoding algorithmic rule includes a higher trust level than a node with a weaker encoding algorithmic rule.

4.3 SMTP

The Simple Mail Transfer Protocol service provided by IIS could be an easy element for delivering outgoing email messages. Delivery of a message is initiated by transferring the message to a chosen SMTP server supported by the domain name of the recipient e-mail address, the SMTP server initiates communications with a Domain Name System (DNS) server, that appearance up then returns the hostname of the destination SMTP server for that domain. Then the originating SMTP server communicates with the destination SMTP server directly through Transmission Control Protocol/Internet Protocol (TCP/IP) on port twenty-five. If the user name of the recipient e-mail address matches one amongst the licensed user accounts on the destination server, the initial e-mail message is transferred to that server, expecting the recipient to choose up the message through a client program. In the case wherever the originating SMTP server cannot communicate directly with the destination server, the SMTP service will transfer messages through one or a lot of intermediate relay SMTP servers. A relay server receives the initial message then delivers it to the destination server, or redirects it to a different relay server. This method is continued till the message is delivered or a chosen timeout period passes. The SMTP service isn't installed by default.

4.4 SMTP vs Mail retrieval

SMTP could be a delivery protocol only. It cannot pull messages from a far-off server on demand. Alternative protocols, like the Post workplace Protocol (POP) and also the internet Message Access Protocol (IMAP) area unit specifically designed for retrieving messages and managing mailboxes. However, SMTP includes a feature to initiate the mail queue process on a far-off server so the requesting system could receive any messages destined for it (see Remote Message Queue beginning below). POP and IMAP are the most popular protocols once a user's pc is barely intermittently powered up, or internet property is barely transient and hosts cannot receive messages throughout off-line periods. Remote Message Queue beginning could be a feature of SMTP that allows a far-off host to begin the process of the mail queue on a server thus it should receive messages destined to that by sending the flip command. This feature but was deemed insecure associated was extended in RFC 1985 with the ETRN command that operates a lot securely using an authentication methodology supported by domain name System data.

4.4.1 Outgoing mail SMTP server

An e-mail client must recognize the IP address of an SMTP server and this needs to tend as a part of its configuration (usually given as a DNS name). The server can deliver outgoing messages on behalf of the user.

4.4.2 Outgoing mail server access restrictions

Server administrators got to impose some control on that clients will use the server. This permits them to handle abuse, as an example spam. 2 solutions are in common use: In the past, several systems obligatory usage restrictions by the situation of the client, solely allowing usage by clients whose IP address is one that the server administrators control. Usage from the other client IP address is disallowed. Modern SMTP servers usually provide another system that needs authentication of clients by credentials before permitting access.

4.4.3 Restricting access by location

Under this method, an ISP's SMTP server won't enable access by users who are 'outside the ISP's network'. a lot of exactly, the server might only enable access to users with an IP address provided by the ISP, that is like requiring that they're connected to the internet using that very same ISP. A mobile user might typically get on a network apart from that of their normal ISP, and can then notice that sending email fails as a result of the configured SMTP server alternative is no longer accessible. This system has many variations. As an example, an organization's SMTP server might solely give service to users on a constant network, implementing this by firewalling to block access by users on the broader internet. Or the server might perform range checks on the client's IP address. These ways were generally employed by firms related to institutions like universities that provided an SMTP server for outward mail only to use internally among the organization. However, most of those bodies currently use client authentication ways, as described below. By limiting access to bound IP addresses, server administrators will readily recognize the IP address of any offender. Because it will be an important address to them, the administrators will handle the rogue machine or user. Where a user is mobile and should use completely different ISPs to attach to the internet, this type of usage restriction is heavy, and fixing the organized outbound email SMTP server address is impractical. It's extremely desirable to be ready to use email client configuration information that doesn't ought to modification.

4.4.4 Client authentication

Modern SMTP servers generally require authentication of clients by credentials before permitting access, rather than limiting access by location as represented earlier. This additional versatile system is friendly to mobile users and permits them to own a fixed selection of organized outbound SMTP server

4.5 Protocol Overview

SMTP is a connection-oriented, text-based protocol within which a mail sender communicates with a mail receiver by issue command strings and provide necessary data over a reliable ordered information stream channel, generally a Transmission Control Protocol (TCP) connection. An SMTP session consists of commands originated by the associate SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) in order that the session is opened, and session parameters area unit changed. A session may embrace zero or additional SMTP transactions. An SMTP transaction consists of 3 command/reply sequences (see example below.) They are: MAIL command, to determine the address, a.k.a. Return-Path, 5321. From, mfrom, or envelope sender this can be the address for bounce messages. **RCPT** command, to determine a recipient of this message. This command is often issued multiple times, one for every recipient. These addresses are a part of the envelope. **DATA** to send the message text. This can be the content of the message, as against its envelope. It consists of a message header associated with a message body separated by an empty line. DATA is truly a bunch of commands, and also the server replies twice: once to the information command correct, to acknowledge that it's able to receive the text, and also the second time when the end-of-data sequence, to either settle for or reject the complete message. Besides the intermediate reply for information, every server's reply will be either positive (2xx reply codes) or negative. Negative replies will be permanent (5xx codes) or transient (4xx codes). A rejection may be a permanent failure by an SMTP server; during this case, the SMTP consumer ought to send a bounce message. A drop could be a positive response followed by message discard instead of delivery. The initiating host, the SMTP consumer, are often either an end user's email consumer, functionally known as a mail user agent (MUA) or a relay server's mail transfer agent (MTA), that's an SMTP server acting as an SMTP consumer, within the relevant session, to relay mail. Absolutely capable SMTP servers maintain queues of messages for retrying message transmissions that resulted in transient failures. An MUA is aware of the outgoing mail SMTP server from its configuration. An SMTP server acting as a consumer, i.e. relaying, usually determines that SMTP server to attach to by trying up the MX (Mail exchange) DNS resource record for every recipient's name. Conformant MTAs (not all) fall back to a square. A record just in case no MX records are often found. Relaying servers may be organized to use a wise host. An SMTP server acting as a consumer initiates a protocol association to the server on the "well-known port" selected for SMTP: port 25. MUAs ought to use port 587 to attach to an MSA. The most distinction between an MTA associated with an MSA is that SMTP Authentication is necessary for the latter solely.

4.6 Algorithm

Assume that a hash function selects each array position with equal probability. If *m* is the number of bits in the array, and *k* is the number of hash functions, then the probability that a certain bit is not set to 1 by a certain hash function during the insertion of an element is then

$$1-\frac{1}{m}$$

The probability that it is not set to 1 by any of the hash functions is

$$\left(1-\frac{1}{m}\right)^{k}$$

If we have inserted n elements, the probability that a certain bit is still 0 is

$$\left(1-\frac{1}{m}\right)^{kn}$$

As a result, the probability that it is 1 is

$$1-\left(1-\frac{1}{m}\right)^{kn}$$

Now evaluate if an entity that isn't in the set is a member. The probability of each of the k array positions computed by the hash functions is 1. The probability of all of them being 1, causing the algorithm to incorrectly say that the element is in the set, is commonly expressed as

$$\left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^{k} = \left(1-e^{-kn/m}\right)^{k}$$

This isn't strictly true since it implies that the probabilities of each bit being set are independent. However, we can assume that the likelihood of false positives decreases as m (the number of bits in the array) increases and increases as n (the number of inserted elements) increases, assuming it is a close approximation. The value of k (the number of hash functions) that reduces the number of hash functions for a given m and n then the probability is

$$\frac{m}{n}\ln 2 \approx 0.7\frac{m}{n}$$

which gives the probability of a false positive of $2^{-k} \approx 0.6185^{m/n}$

The necessary number of bits m can be calculated by substituting the optimal value of k in the probability expression above, given n (the number of inserted elements) and a desired false positive probability p (assuming the optimal value of k is used):

$$p \approx \left(1-e^{-(m/n\ln 2)n/m}\right)^{(m/n\ln 2)}$$

which can be reduced to:

$$\ln p = -\frac{m}{n}(\ln 2)^2$$

As a result of this,

$$m = -\frac{n\ln p}{(\ln 2)^2}$$

This implies that the length of a Bloom filter m is proportional to the number of elements filtered n for a given false positive probability p. [two] While the above formula is asymptotic (that is, applicable as m, n), the agreement with finite values of m, n is also very good; the false positive probability for a finite bloom filter with m bits, n components, and k hash functions is at most 1%.

$$\left(1-e^{-k(n+0.5)/(m-1)^k}\right)$$

Hence, if we need to pay a penalty for at most half an extra element and at most one less bit, we can use the asymptotic formula.

V. RESULTS AND DISCUSSION

5.1 Results of Descriptive Statics of Study Variables

Obtaining the result of home page size and download season of landing page of different mail administrations considering the setup C1 and the outcomes are introduced in Table 1. From this Table 1, it is seen that, if the picture size is high, the download time is likewise relatively high. The section Image size/Code size gives fascinating perceptions. For Hotmail, despite the fact that the extent of picture size to HTML code size is high, the measure of information downloaded each second is less, contrasted with Rediffmail. The relationship between the home page measure and download time is assessed, and the estimation of connection coefficient (r) is acquired as 0.98. It shows that both are exceptionally related.

Table 1 Comparision of various Mail Servers

Mail Service	HTML Code Size	Image Size (kb)	page size (kb)	Download time	pz/d t	Image size/ Code size
Gmail	25	6.63	31.63	10.09	3.14	0.27
Rediffmail	44	76.8	120.8	19.85	6.09	1.75
Hotmail	14	192	206	43.76	4.71	13.71
Yahoo	175	341	516	253.78	2.03	1.95
FEDS MailServer	15	5.5	30.9	9.0	2.90	1.55

Table 2 Comparision of Various Protocols

Algorithm	Result Generation	Accuracy	Result Suggestion
SMTP	**90 Sec**	**90 %**	**79%**
HUIAR	**45 Sec**	**92 %**	**85%**
ESMTP - TaaS	**30 Sec**	**97 %**	**99 %**

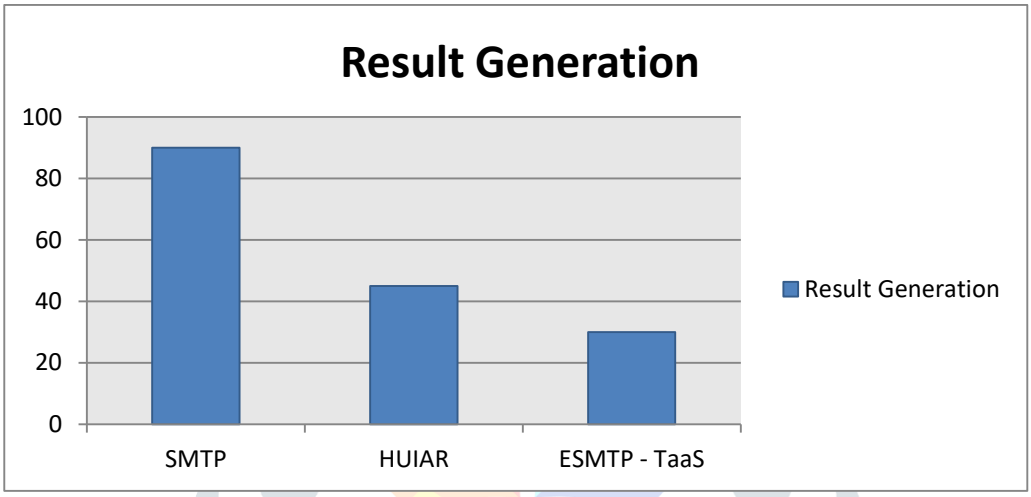

Fig.2 Result Generation

V. ACKNOWLEDGMENT

Working on this project "Advanced Mail Server Using Fire Eye Detection System" was a source of immense knowledge to us. We would like to express our sincere gratitude to Mrs.K.Mouthami for her guidance and valuable support throughout the project. We are very thankful to the Department of Information Technology for providing the golden opportunity to work on this project.

REFERENCES

1) W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collecting in smart city," IEEE Transactions on Industrial Informatics, p. 1, 2020.

2) A. Rani and S. Kumar, "A survey of security in wireless sensor networks," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-5.

3) H. Fouchal, J. Biesa, E. Romero, A. Araujo and O. N. Taladrez, "A Security Scheme for Wireless Sensor Networks," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-5.

4) Udhayavani, M., & Chandrasekaran, M. (2018). Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: A trust-aware routing framework for wireless sensor networks. Cluster Computing,22, 11919–11927.

5) Kong, L., Pan, J. S., Snášel, V., Tsai, P. W., & Sung, T. W. (2018). An energy-aware routing protocol for wireless sensor network based on genetic algorithm. Telecommunication Systems,67(3), 451–463.

6) Zlomislic, V., Fertalj, K. & Sruk, V. Denial of service attacks, defences and research challenges. Cluster Comput 20, 661–671 (2017).

7) Manish Patel, Akshai Aggarwal and Nirbhay Chaubey, "Wormhole Attacks and Countermeasures in Wireless Sensor Networks: A Survey", International Journal of Engineering and Technology, vol. 9, no. 2, pp. 1049-1060, April 2017.

8) Muhammad Noman Riaz et al., "Classification of Attacks on Wireless Sensor Networks: A Survey", International Journal of Wireless and Microwave Technologies, vol. 6, pp. 15-39, November 2018.

9) Saurabh Sharma and Sapna Gambhir, "CRCMD&R: Cluster and Reputation based Cooperative Malicious node Detection and Removal Scheme in MANETs", IEEE 11th International Conference on Intelligent Systems and Control, pp. 36-340, 5–6 Jan 2017.

10) Xinyang Zhang and Jidong Wang, "An Efficient Key Management Scheme in Hierarchical Wireless Sensor Networks", ICCCS IEEE, 2015

11) H. Xie, Z. Yan, Z. Yao and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey", IEEE Internet Things J., vol. 6, no. 2, pp. 2205-2224, 2019.

12) M. A. Siddiqi, A. A. Mugheri and M. Khoso, Analysis on Security Methods of Wireless Sensor Network, vol. 2, no. 1, 2018.

13) 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.

14) S. Umba, Masengo Wa, Adnan M. Abu-Mahfouz, T. D. Ramotsoela and Gerhard P. Hancke, "A Review of Artificial Intelligence Based Intrusion Detection for Software-Defined Wireless Sensor Networks", 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), pp. 1277-1282, 2019.

15) Manal A. Abdullah, Bdoor M. Alsolami, Hana M. Alyahya and Maha H. Alotibi, "Intrusion detection of DoS attacks in WSNs using classification techniuqes", Journal of Fundamental and Applied Sciences, vol. 10, no. 4S, pp. 298-303, 2018.

16) Rakesh Sharma and Vijay Anant Athavale, "Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks", International Journal of Advanced Networking and Applications, vol. 10, no. 4, pp. 3925-3937, 2019.

17) J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," IEEE Access, vol. 7, pp. 33859–33869, 2019.

18) D. C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust," Cluster Computing, vol. 22, no. S1, pp. 1313–1328, 2019.

19) Jayashree Agarkhed, Gauri Kalnoor and Siddarama R. Patil, "Intrusion Detection System Using Pattern Matching Techniques for Wireless Sensor Networks" in Innovations in Computer Science and Engineering, Singapore:Springer, pp. 411-418, 2019.

20) Elie Kfoury, Julien Saab, Paul Younes and Roger Achkar, "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks", International Journal of Interdisciplinary Telecommunications and Networking (IJITN), vol. 11, no. 1, pp. 30-43, 2019.

21) R. Maidhili and G. M. Karthik, "Intrusion Detection and Prevention Based on State Context and Hierarchical Trust in Wireless Sensor Networks", 2018 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-8, 2018.