Server Monitoring System Using A Network Intelligent Agent

Mrs.S.Rajanandini[1], Ms.R.Aishwarya[2], Ms.M.Akshaya[3]
[1, 2, 3] Dept of BCA & M.Sc. SS
[1, 2, 3] Sri Krishna Arts and Science College, Kuniamuthur, Coimbatore-8

Abstract- *Server monitoring is the process of reviewing and analyzing a server for availability, operations, performance, and security purpose. Server plays the administrator role to ensure the performance of network and to mitigate problems, if any. A secure server monitoring system is achieved using a network intelligent agent. To develop a Network Intelligent Agent which does two tasks, first task is named as Network Alert System in that the server monitoring system monitors the health of server and a notification message is sent to registered users. The monitoring system verifies the status of the server by sending heart beat message. The system is responsible for maintaining the list of users to which the notification has to be sent when the server goes down. If the server goes offline, the system alerts the server by sending notification message to the registered mobile devices and to the mail address. Second task is Network Authenticated Mechanism based on CFP (Computer Finger Print), for Networks that fulfils the requirements of security. To identify CFP, machine id is generated and a cryptographic license key from a server is obtained, and then each time the program runs check the machine's fingerprint against the one stored in the license file. The CFP is used for authentication purpose to avoid unauthorized users to access the server database. Machine id has a hardware serial number. This includes the CPU, each of the hard disks, and all the network interfaces, which each have a globally unique MAC address. Using an intelligent agent it helps to find and filter information on surfing the Internet and provides a secure server network monitoring system.*

Keywords- CFP, Cryptographic license key, Intelligent Agent, MAC address.

I. INTRODUCTION

Server monitoring system monitors system resources like CPU Usage, Memory Consumption, Input Output devices, Network, and Disk Usage. Server monitoring is basically a preventative measure that helps to detect any issues before they cause any major issues that affect the server network. Server monitoring system continuously monitorsthe server to its designated network for any failures or any irregularities that are detected by server monitoring software due to network crash.Nowadays, managing the increasing number of servers with the limited resources is a big challenge for server monitoring. As soon as one server cluster gets up and running, there is need to setup another one. But with the limited number of resources in the organization, server management and monitoring becomes difficult.For this cause a Network Intelligent Agent is developed to provide secure server monitoring.

Network Intelligent Agent does two tasks, first oneis Network Alert System in which server monitoring system monitors the health of server and a notification message is sent to registered users. The monitoring system verifies the status of the server by sending heart beat message. If the server goes offline, the system sends notification message to the registered mobile devices and to the mail address. The system will send notification message to all the users registered to receive notification message. The system alerts the accurate server since it maintains the list of users to which the notification has to be sent when the server goes offline. The notification alert message is sent in an ICMP (Internet Control Message Protocol) message format. It alerts the server and sends notification by checking all the server details with the main server. If one server goes down the system checks for its details and monitors that particular server and sends notification. These details verification follows the second task.

Second task is Network Authenticated Mechanism based on CFP (Computer Finger Print), for networks that fulfil the requirements of security. Each system has its own CFP, it differs from one another. With this unique machine finger print it provides ease way of alerting the server. To identify CFP generate a machine id, get a cryptographic license key from a server, and then each time the program runs check the machine's fingerprint against the one stored in the license file. The main use of CFP is for authentication purpose to avoid unauthorized users to access the server database. Machine id has a hardware serial number. This includes the CPU, each of the hard disks, and all the network interfaces, which have a globally unique MAC address.The computer finger print (CFP) denotes the MAC address of each system since it is unique from each other. During monitoring the CFP verification for each system is processed, and if any system goes offline an ICMP message alert is sent to the server. This proposed scheme provides data authentication, confidentiality and integrity in Networks. Using an intelligent agent it helps to find and filter information on surfing the internet and provides secure monitoring.

II. SERVER MONITORING PERFORMANCE

Server monitoring work plays a prominent role in saying that nowadays there are lots of companies with rather small and simple networks where servers are also used and needed to be monitored. A sever is monitored to keep the data safe and secured. A key reason for monitoring is troubleshooting server performance problems. For example, users mayhave problems connecting to the server and this case need to monitor the server to troubleshoot these problems. Another common reason for wanting to monitor a server is to improve server performance. High server performance is obtained by improving the Input Output disk, reducing CPU usage, and cutting down on the network traffic load on the server. For example, as the number of users accessing a server grows, in that cause its not be able to reduce the network traffic load, so server performance is improved through load balancing or by distributing key data files on separate drives.

So the first job for a system or server admin is to wonderabout the need to be monitored. Depending on the application that the server is running, there will be mission-critical service some require built-in OS services to run in addition to their services and some only require their own services. Knowing application of the server in which it runs, there are a set of basic components that must be monitored.

2.1 Basic Components

2.1.1 CPU

The CPU is the brain of the server hardware. The Central Processing Unit (CPU) is the portion of a computer system that carries out the instructions of a computer program, to perform the basic arithmetical, logical, and input/output operations of the system. A server that has its CPU pegged 100% for several minutes, or even hours is an unhappy server. This means that the server has no time (cycles) to service additional requests to find they are mission-critical or not. Based on the cause of the CPU spike, to recover damages server have to either upgrade the CPU hardware, add more CPU’s or shut down frivolous services that are hogging these critical resources. If a server CPU is always at 75% or higher usage, one of the above suggested steps are need to be considered during monitoring.

2.1.2 RAM

Random Access Memory (RAM) is a form of data storage. A server can load information required by certain applications into RAM for faster access thereby improving the overall performance of the application. This is because the RAM is flash based storage and is several times faster than the slower hard disk. If a server runs out of RAM, it sets up a portion of the hard drive as virtual memory and this space is reserved for CPU usage.This process is named as swapping and thus causes performance degradation since the hard drive is much slower than RAM. Swapping also contributes to file system fragmentation which degrades overall server performance. Soif RAM usage is constantly rising, needed to add more RAM for a cheap way to boost server performance.

2.1.3 Hard Disk

The hard disk is the device that the server uses to store data. The inbuilt hard disk drive consists of several rigid rotating discs coated with magnetic material with magnetic heads arranged strategically to write data to, and read from the disc or platter. The data stored are permanent and non-volatile and are available till it is consciously erased by the end user. It is the need to monitor the hard disk because the operating system needs space on the disk for normal operating processes including paging files and certain caches. The application running on the server must need space to write temporary data for efficient operation and also need space for permanent data accessed by the user. This low free space on a drive is one of the reasons for file system fragmentation which causes severe performance issues.

2.2 Hardware Components

2.2.1 CPU Fan

This fan draws heat away from the CPU. The process of this fan is to draw cooler air into the case from the outside, expel warm air from inside, or move air across a heat sink to cool a particular component. If the CPU fan fails, either the server will eventually overheat and fail or perform an emergency shutdown to prevent serious damage thus the server becomes unavailable. To prevent this from happening, CPU Fan speed-monitor RPM (revolutions per minute) is monitored in safe levels. If there is a spike in fan RPM that lasts several minutes or hours, that is an indicator of a serious issue. For example, if the AC is not working, the fan vents are blocked.

2.2.2 Temperature

The temperature of the motherboard is another important hardware component to be monitored. Unusually high temperatures can cause permanent damage to the server and will affect server performance adversely. So a safe working temperature limits are obtained from the manufacturer and monitored within a safe range. With the addition of virtualization to the mix, server density has increased. This makes monitoring temperatures both internal server and external server environment even more critical. In this case,temperature measurements are used to plan and deploy virtual servers for appropriate monitoring. For example, a high load web or database server is not be deployed on a physical server since it is approaching temperature limits for safe operation.

III. SERVER MONITORING CHALLENGES

A one big challenge for server monitoring is managing the increasing number of servers with the limited resources. As soon as one server get cluster there is a need to setup another one. But it is not possible with the limited number of resources in the organization, so thus the server management and monitoring becomes difficult. Even in IT infrastructure with growing number of servers also becomes heterogeneous. Different servers have different operating systems and thus the server need different methods for implementation and monitoring.

It is also important that the Server Monitoring gains deep service level insights into the systems for a complete monitoring. And it must be able to ensure that the system is functionally stable and working efficiently to win over this challenge. Server monitoring helps in effective management of resource utilization during the over load of hardware resources on the server, that marks another challenge for server monitoring to give insights into the resources.

IV. IMPORTANCE OF SERVER MONITORING

Any network crashes it costs time and money to fix. At a time of downtime that is already costing the business money and hurting its reputation, it will be difficult to fork out more cash to get things back up and running again. Here theServer monitoring is important thatcan monitor any small issues before they evolve into anything major. Server monitoring is essential in ensuring service availability. The basic concept of server monitoring is to ensure a server or server infrastructure is functioning as it should be, but many stop monitoring at this stage. So it is important to understand effective server monitoring allows to take this is a step further to enable effective performance testing to overcome any issues with the server.

Server monitoring involves monitoring many different aspects of a network or server infrastructure. The server hardware, operating system, applications running on the operating system, network traffic, memory and disk utilization and CPU usage are examples of top level items monitored in a common server infrastructure. In more depth, monitoring can be performed in disk queue length, memory pages per second and total network bytes per second. Many other application or hardware specific monitoring can be configured and setup depending on which pieces of information is critical to business and support needs.

In business today it is very important to understand the importance of real time monitoring. This enables user to establish important statistics of server, network and application performance. Real time monitoring not only gives accurate note on good or bad network environment but also hugely helps with foreseeing any future possible issues which the network might face as well as troubleshoot any on-going support work required. Effective real time monitoring not only is crucial to most business because monitoring system ensures functionality properly but also saves businesses money in the long run if any application/server downtime occurs it wouldn’t be difficult for the server environment to trace the issues happened before.

V. DEVELOPING A NETWORK INTELLIGENT AGENT

Network Intelligent Agent is developed to monitor the server from multiple locations.This provides a secure monitoring. Server is monitored usually when the users have problem in connecting to the server due to network issues and also monitored to gain high performance. To have a secure server monitoring, a network intelligent agent is developedwhich does two tasks, first one is Network Alert System in that server monitoring system monitors the health of the server and a notification message is sent to registered users.Second one is Network Authenticated Mechanism based on CFP (Computer Finger Print), for networks that fulfill the requirements of security. Here the CFP indicates the MAC address of the system.

5.1 Network Alert System

Monitoring is a mechanism that oversees system issues, business activities, and integration processes. The sole purpose of the monitor is to raise alerts based on predefined rules. The alerts may indicate any problems, network failure, or errors that should be recovered are sent to the server. During a multiple connection to the server, monitoring systemmonitors the health of server and a notification message is sent to registered users. The monitoring system verifies the status of the server by sending heart beat message. If the server goes offline, the system sends notification message to the registered mobile devices and to the mail address. The system will send notification message to all the users registered to receive notification message. The details of the entire server are registered into the main system by which the system can monitor the server and sends notification message through a SMS or email. Here ICMP (Internet Control Message Protocol) message format is used to send SMS alert to the server.

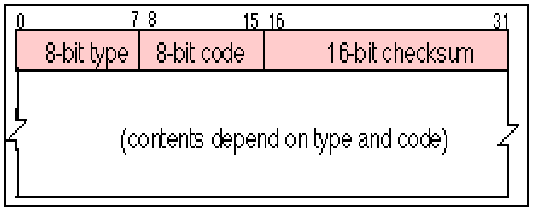

Figure 1. Format of an ICMP message

. ICMP message is sent to alert the server for a secure network alert. The Internet Control Message Protocol (ICMP) is a best example of a client server application. The ICMP server executes on all IP end system computers. The protocol is used to report problems with delivery of IP datagram within an IP network. It can be used to show when a particular server is not responding due to unreachable of an IP network. The ICMP message is sent to correct destination server by setting the source address to the address of the computer that generated the IP packet and the IP protocol type is set as "ICMP" to indicate that the packet is to be handled by the remote end system's ICMP client interface.

The ICMP protocol has the ability to control and provide a secure network alert to the server. Because of the capability of ICMP, to affect the operation of important system functions and obtain configuration information, hackers have used ICMP messages in a large number of attacks. As a result of concerns about such attacks, network administrators often arrange to block ICMP messages with firewalls. If ICMP is blocked, a number of common diagnostic utilities like ping, traceroute do not work properly. To overcome from this issue the intelligent agent work on second task, Network Authenticated Mechanism based on CFP (Computer Finger Print). The CFP detail of entire system is registered to the main server, when server is monitored it checks and verifies the details of all the registers users. If one server goes down during monitoring the ICMP message is then sent to the server after CFP verification.

5.2 Network Authenticated Mechanism

Network Authenticated Mechanism is based on CFP (Computer Finger Print), for Networks that fulfils the requirements of security. In server monitoring the CFP is used for authentication purpose to avoid unauthorized users to access the server database. Since, a computer finger print is unique for each system all over its ease way of obtaining a secure monitoring. To identify CFP of each system generate a machine id, get a cryptographic license key from a server, and then each time the program runs check the machine’s fingerprint against the one stored in the license file.Machine id has a hardware serial number. This machine id includes the CPU, the hard disks, and all the network interfaces, each of which have a globally unique MAC address.The MAC address of each system is stated as a computer finger print this it is unique as human finger print. These CFP details of each system are registered into the server. If a server goes offline during monitoring, the ICMP message is then sent to the server after CFP verification. It helps in understanding server’s system resource usage that provides a better end-user experience.

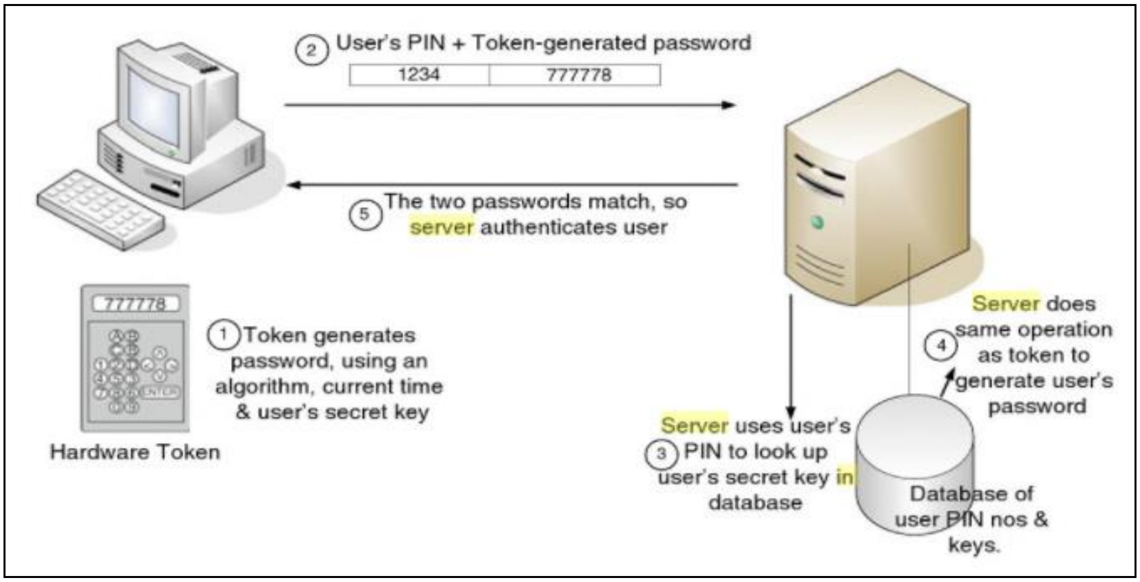
2 User's PIN + Token-generated password
1234
777778
5 The two passwords match, so server authenticates user
777778
1 Token generates password, using an algorithm, current time & user's secret key
Hardware Token
Server does
4 same operation as token to generate user's password
Server uses user's
3 PIN to look up user's secret key in database
Database of user PIN nos & keys.

Figure 2. Time-synchronous authentication

Network Authentication Mechanism provides a safer form of authentication by using an intelligent token (hardware token) that generates a one-time password. This password is transmitted to a secure server that verifies it and allows the user to log in. This hardware token is specified as unique computer finger print of a system. There are two forms of intelligent token: time synchronous and challenge response. In a time synchronous system, the token and the server have to be synchronized. A random number is generated roughly once per minute by both the server and the token. To log into a server, a user has to enter a personal identification number plus random number that the hardware token displays. In a challenge response system, users have to supply an encrypted number that is the same as the one that the server has generated for authentication. Since all the details of the system are stored in the database, the server and the user provide a secure authentication. Authorization allows administration to control over the network resources. The administrator has to monitor the security mechanisms for the better growth of the server. Once authentication is completed the monitoring system alerts the server by sending ICMP message if there any network issue. This entire process of Network Intelligent Agent proves a better way for a secure server monitoring.

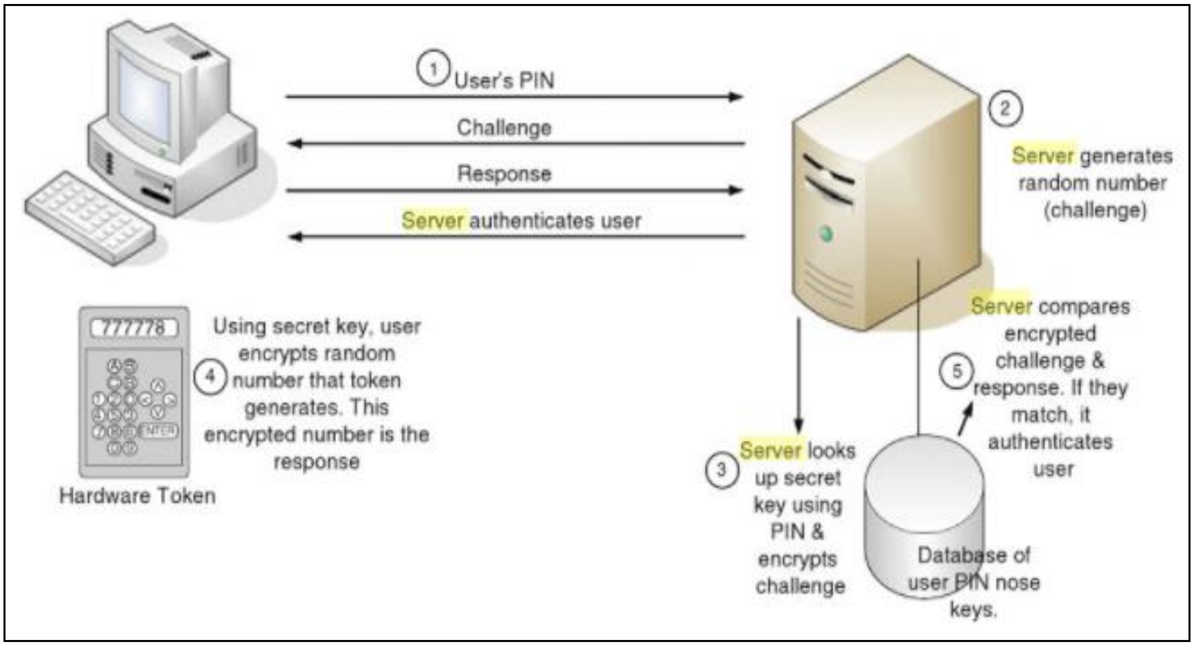
1 User's PIN
Challenge
Response
Server authenticates user
2
Server generates random number (challenge)
777778
4 Using secret key, user encrypts random number that token generates. This encrypted number is the response
Hardware Token
Server compares encrypted challenge & response. If they match, it authenticates user
5
3 Server looks up secret key using PIN & encrypts challenge
Database of user PIN nose keys.

Figure 3. Challenge-response authentication

VI. CONCLUSION

In this paper, a system which follows distributed and decentralized approach for the purpose of server monitoring and management is proposed for the purpose of reducing the traffic over the network.It is safe to say that most businesses rely heavily on the stability of their IT network and infrastructure and it is a fact that the cost of downtime is becoming an increasingly growing concern. The network downtime not only causes a major loss of business productivity but also affects the quality of service that is provided to the customer and impact of service given by the organization can also cause severe damage to the business reputation. For this case the server monitoring is developed and now plays a most prominent role in protecting the business and its reputation.

Here Server Monitoring is widely protected for a reason to secure all the data and user information stored in the server. Network Intelligent Agent is one such new technology used to provide a secure networking. It works on computer finger print, since in whole world a finger print of all humans doesn’t match with one another. Likewise, computer finger print differs for each system and it can never be same. This provides server with a secure monitoring.

REFERENCES

[1] Larkins Carvalho and Nielet D’mello, “Secure network monitoring system using mobile agents”, International Journal of Modern Engineering Research (IJMER), vol. 3, issue. 3, (2013), pp. 1850-1853.

[2] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Muhammad Inayatullah Babar, “An Efficient Network Monitoring and Management System”, International Journal of Information and Electronics Engineering, vol. 3, no. 1, (2013).

[3] Prof.B.Murali and Ms.A.Mary Subasree, “System Intelligent Agent in Distributed Computing”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue. 8, (2015).

[4] L. Chang, W.L. Chan, J. Chang, P. Ting, M. Netrakanti, “A network status monitoring system using personal computer,” presented at IEEE Global Telecommunications Conference, August (2002).

[5] John Cowley, “Communications and Networking: An Introduction”,second edition.