Intrusion Detection System Using Cloud Computing

Vipul Singh
B.Tech Computer Science and Engineering
Amity School of Engineering & Technology
Noida, Uttar Pradesh
Vipul074@gmail.com

Shikhar Seth
B.Tech Computer Science and Engineering
Amity School of Engineering & Technology
Noida, Uttar Pradesh
Shikhars335@gmail.com

Deepak Gaur
Assistant Professor
Amity School of Engineering & Technology
Noida, Uttar Pradesh
dgaur@amity.edu

Abstract— This paper indicates how we can spare secret information from an interloper or any sort of spillage of the information by utilizing private cloud and dab net advancements With the expanding notoriety of distributed computing idea and its accessibility empowers increasingly association to change their condition to cloud based condition. This paper manages the security of information or any record which association need to keep that classified or mystery through cloud administrations with simple equipment necessity and along these lines remotely getting to every one of those applications introduced on the arrangement of the association and just chose mac address locations will given the rights to download that document from private cloud and get to that record, likewise alluded as "Information security" in the paper. This approach can definitely limit the theft of the secret information and furthermore with the expanding utilization of fast web; this idea appears to be more coherent and effective. The application which is utilized for executing this idea is of most extreme significance in light of the fact that here it's the application which specifically communicate with administrations gave by utilizing private cloud. Linux is utilized here due to its security and adaptability. There are couple of more explanations behind picking Linux as it is lightweight and more secure.

Keywords— Cloud, private cloud , data security, intruder detection system, diffie hellman, split and merge, FTP, AES algorithms.

I INTRODUCTION

In the IT business, the expression "security" continued the inclination either its for a report or activities or customer's subtle elements. Utilizing the utilization of information interloper identification we are giving the unique private get to cloud which will be gotten to by those exclusive who have given the rights. Just those mac address locations will be permitted to get to that ip which have advantaged access to it which is given by administrator of the application.

II INTRUSION DETECTION

The purpose of this project is to overcome the security issues pre Mounting world cannot imagine even for a single day without computer and computer is basis on internet. Nowadays secure information of internet is becoming very high priority. Modern world emphases in a way by which it can be protect the data and information from any illicit and unauthorized access. Intrusion Detection Systems (IDS) can be differs in various techniques and advance with the objective to detect suspicious traffic in dissimilar ways. There are two significant categories of intrusion detection systems. One is called network-based intrusion detection system (NIDS) and the other one is host-based intrusion system (HIDS). Intrusion detection system (IDS) can be differs in various techniques and advance with the objective to detect suspicious traffic in dissimilar ways. There are two significant categories of intrusion detection systems. One is called network based intrusion detection system(NIDS) and the other one is host-based intrusion system (HIDS).

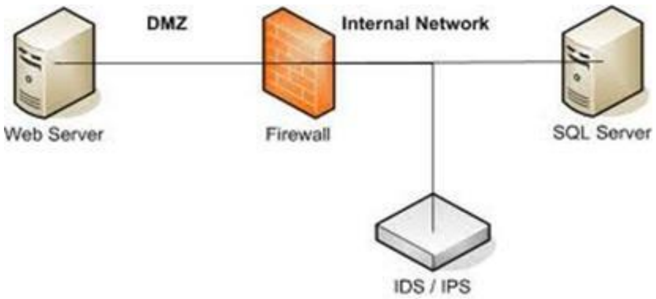

Fig 1 IDS SYSTEM

III ALGORITHMS USED

AES Algorithm for encryption: AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

FTP for file transferring: The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files from a server to a client using the Client–server model on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

Diffie hellman : Diffie–Hellman key exchange (D–H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Diffie–Hellman is used to secure a variety of Internet services.

Split and merge algorithm: split and merge algorithm is used for dividing a file or document in the parts with a some pattern for e.g. which starts from the A and ends from Z than if we divide it in to two parts than one part will have a pattern which starts from A and ends with H than the second part will start from I and end from Z and merge performs a task of joining both parts according to the continuation of the file pattern

IV PROPOSED MODEL:

Work Cloud computing provides application and storage services on remote servers: The clients do not have to worry about its maintenance and software or hardware up-gradations. Cloud model works on the „concept of virtualization‟ of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine. Deploying HIDS in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the rapid flow of high volume of data as in cloud model, there would be issues of performance like overloading of VM hosting IDS and dropping of data packets. Also if host is compromised by an offending attack the HIDS employed on that host would be neutralized. In such a scenario, a network based IDS would be more suitable for deployment in cloud like infrastructure. NIDS would be placed outside the VM servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. Such NIDS would still be facing the issue of large amount of data through network access rate in cloud environment. To handle a large number of data packets flow in such an environment a multi-threaded IDS approach has been proposed in this paper.

The multi-threaded IDS would be able to process large amount of data and could reduce the packet loss. After an efficient processing the proposed IDS would pass the monitored alerts to a third party monitoring service, who would in turn directly inform the cloud user about their system under attack. The third party monitoring service would also provide expert advice to cloud service provider for mis-configurations and intrusion loop holes in the system. proposed multi-threaded NIDS model for distributed cloud environment is based on three modules: capture & queuing module, analysis/ processing module and reporting module. The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets.

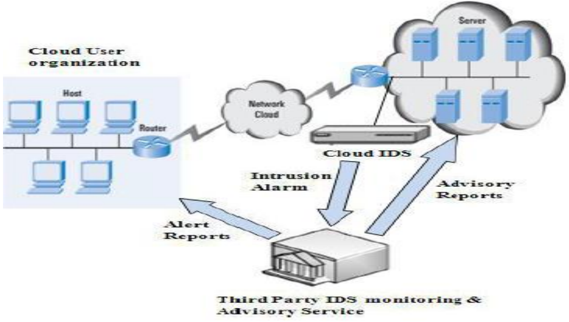

fig 2 proposed model

V REQUIREMENT OF A SERVER

All servers have certain base particulars:
Equipment Network (Infrastructure): The server PC needs to be fitted with a specific measure of equipment particulars contingent upon the likely number of clients and the measure of information to be put away in the system. The bigger the quantity of clients and the measure of information to be put away, bigger is the server limit and the other way around.

Working System (Platform): Without an Operating System, no machine can run. Consequently, a working framework must be introduced in the server PC according to the prerequisite of the client. Microsoft Windows Server 2008 is an ordinarily utilized Operating System in different Server Computers.
Applications (Software): The virtual products introduced in the Operating System, similar to business applications as ERPs. These programming projects are the general and the essential virtual products required by the customer PCs for their work purposes.
Methods of Services offered inside Cloud Computing [1][4]:
At business level, the three methods of administrations might be delegated under [2]:
1. IaaS, i.e. Just Infrastructure.
2. PaaS, i.e. Framework and Platform.
3. SaaS, i.e. Framework, Platform and Software.
APPLICATION AS A SERVICE

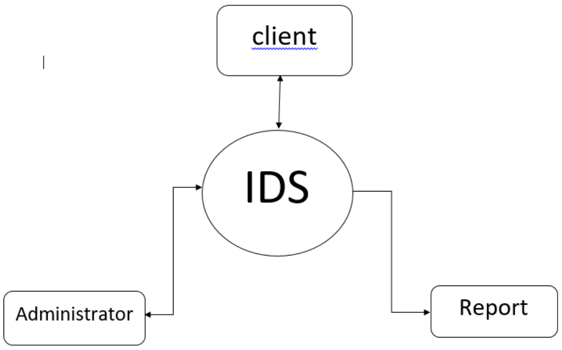

Fig 3 Context level DFD

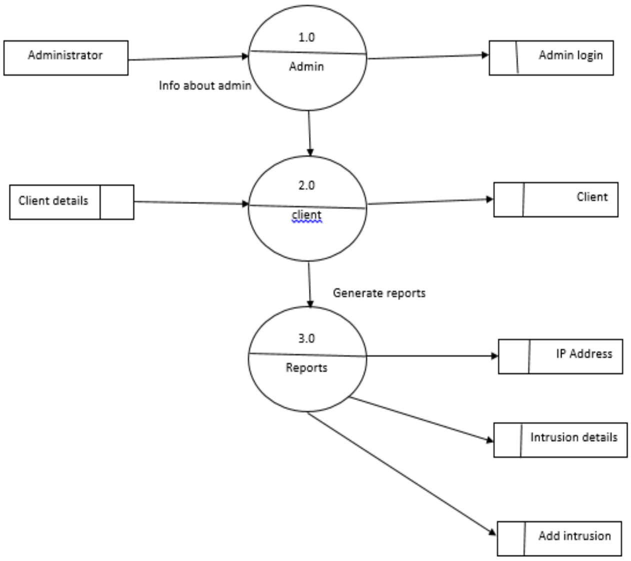

Fig 4. Data flow diagram

As a rule, Saas [5] permits client to utilize effectively existing on the web applications. A regular case of Saas is taking a shot at spreadsheets and word archives on Google itself. Applications like Snapchat and Whatsapp are additionally some important cases of Softwares as a Service. It is open from any PC and is accessible on either free or paid membership in light of the vendor[5].

PLATORM AS A SERVICE

It essentially hands over a toolbox or an appropriate domain to the client for making new arrangements of online applications according to his own particular prerequisite. As a typical case, Google's App Engine gives a positive domain to the client to make his coveted new programming utilizing the effectively present Google's Infrastructure. By and large, these administrations are given with ease and subsequently are viewed as exceptionally convenient for the clients. It confines the client to utilize those programming dialects and instruments which their stage supplier has not given

INFRASTRUCTURE AS A SERVICE

It permits an undertaking to run whatever administration it requires on a cloud equipment. In basic terms, Infrastructure as an administration essentially includes the equipment related administrations that is given to the client by a cloud merchant. These by and large incorporate Virtual Servers or possibly a sort of capacity gadget [4]. Here, the basic applications possibly moved from the endeavor's server farm to the cloud specialist co-op keeping in mind the end goal to lessen IT costs. It essentially hands over a toolbox or a reasonable domain to the client for making new arrangements of online applications according to his own particular necessity. As a typical illustration, Google's App Engine gives a great situation to the client to make his coveted new programming utilizing the officially present Google's Infrastructure. By and large, these administrations are given requiring little to no effort and consequently are viewed as exceptionally convenient for the clients. It limits the client to utilize those programming dialects and instruments which their stage supplier has not given.

VI. TYPES OF CLOUD DEPLOYMENT MODEL

Cloud Deployment model is a feature which is defined by the user of the cloud service, and noticeable not the company or the organization offering the cloud service to the user. It is not defined using technology, cost or location factors.

An IaaS is given to the client as a Public or Private Cloud [4].

Public Cloud

Out in the open cloud, the cloud specialist co-op makes the cloud benefit accessible to the client for an expense or perhaps free. Anyone can work upon the gave asset according to his/her own particular utilize. It is an unhindered administration. People in general cloud is associated with open web for anybody to use [4]. It is being considered as somewhat unreliable as the administration is unhindered and substantial quantities of clients are inside the system. Beat two IaaS specialist co-ops are Amazon WS and Rackspace Hosting.

Private cloud

In a private cloud, all capacities of the administration gave utilizing an open cloud are controlled by an endeavor in their own facilitated condition [4]. Its essential component incorporates the way that lone that specific association or endeavor can control it and for its own utilization as it were. These conditions can be associated with a few clients over a private line and subsequently diminishing the danger of security issue over the system. Outstandingly, it can likewise be associated through the general population web. It is more costly than an open cloud benefit.

Hybrid cloud

This cloud gives the best of both open and private cloud. Utilizing this administration, the associations utilize less secure administration over an overall population cloud system and application which required greater security are keep running over the private cloud organize. Cloud blasting is another term identified with half and half cloud. Here, when load gets substantial on the private cloud arrange, the organization utilizes people in general or general cloud for the additional limit requested on a "pay as you utilize" premise. The over-burden on the private system is named as cloud blasting. Cross breed cloud arrange as far as anyone knows named as the cloud innovation without bounds.

VII. CONNECTING TO CLOUD

There are many ways by which a Client can establish a connection with Cloud and can use Cloud services. These two are the most common [2]:

1. Using a software to operate internet
2. Using an application which is built to give services

Previously mentioned application can keep running on PC, server, handheld gadget like versatile and so on. With the above expressed means these all equipment gadgets speak with cloud benefits over an uncertain and temperamental medium. We can set up a safe association between these gadgets and cloud.

VIII BENEFITS AND FUTURE SCOPE OF THE CONCEPT

i. At the time of establishment of an organization which can manage the cost of the utilization of cloud administrations (i.e. can keep up web association all through the association grounds) will be exceedingly profited as they get the opportunity to be more secure. Also, there confidentiality will be maintained.

ii. In the workshops of schools and universities where so many labs with different kinds of LAN connections are managed, can be very much benefited if all computers are under observation of admin with whose help intruder can be avoided from invading the network and performing malicious activities.

iii. This concept can be used at offices of government and other agencies to secure citizens information and maintain integrity of the country. An extremely high internet connection will be provided to all the employers to perform any kind sensitive task bearing some information using the services provided by cloud.

iv. People can also form there own private network and add 10 to 20 people by forming a group where they can share, download, delete files by using services of a private cloud and keep themselves away from intruder by blocking his/her IP address.

IX REFERENCES

1. Sebastian Roschke, Feng Cheng, Christoph Meinel,“ Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
2. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.
3. Andreas Haeberlen,“ An Efficient Intrusion Detection Model Based on Fast Inductive Learning”, Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.
4. Richard Chow, Philippe Golle, Markus Jakobsson, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”, ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.
5. Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.
6. Irfan Gul, M. Hussain, “Distributed cloud intrusion detection model”, International Journal of Advanced Science and Technology Vol. 34, September, 2011.
7. D.Bala Krishna, R.A.Melvin Meshach, “Cloud Computing along Web-OS”,*IJCER*,Pollachi,India,2013
8. Noopur Bardhan, Operating System Used in Cloud Computing *IJCSIT*, International journal of Computer science and information technologies, Vol. 6(1),2015,542-544