AMITY UNIVERSITY

UTTAR PRADESH

Major Project Report
on

Intrusion Detection System Using Cloud Computing

Submitted to
Amity University Uttar Pradesh

In partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

By

VIPUL SINGH

(A2345913028)

Under the guidance of

Mr. Deepak Gaur

Assistant Professor

Department of Computer Science & Engineering

Amity School of Engineering & Technology

Amity University Uttar Pradesh, Noida

May 2017

DECLARATION

I , **Vipul Singh**, student of B.Tech (CSE) hereby declare that the project titled "**Intrusion Detection system using cloud computing**" which is submitted by me to Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, in partial fulfillment of requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

Noida

Date VIPUL SINGH

CERTIFICATE BY THE GUIDE

On the basis of declaration submitted by **Vipul Singh** , student of B.Tech CSE, I hereby certify that the project titled "**Intrusion detection system using cloud computing**" which is submitted to Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering, is an original contribution with existing knowledge and faithful record of work carried out by them under my guidance and supervision.

To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Noida

Date

Mr. Deepak Gaur
Assistant Professor
Department of computer science and engineering
Amity School of Engineering & Technology, Noida

Acknowledgement

I take this opportunity to express my profound sense of gratitude and respect to all those who helped us throughout our project.

This report acknowledges to the intense driving and technical competence of the entire individual that have contributed to it. It would have been almost impossible to complete this project without the support of these people. We extend thanks and gratitude to **Prof. (Dr.) Abhay Bansal,** HOD, Department of Computer Science and Engineering, **Mr. Deepak Gaur**, Assistant Professor**,** Department of Computer Science and Engineering who have imparted me the guidance in all aspects. They shared their valuable time from their busy schedule to guide me and provide their active and sincere support for my activities.

This report is authentic record of my own work which is accomplished by the sincere and active support by all the teachers of my college. I have tried my best to summarize this report.

Vipul Singh
B. Tech CSE
Amity School of Engineering and Technology, Noida
2013-2017

Abstract & Keywords

This paper shows how we can save confidential data from an intruder or any kind of leakage of the data by using private cloud and dot net technologies . With the increasing popularity of cloud computing concept and its availability encourages more and more organization to switch their environment to cloud based environment. This paper deals with the security of data or any file which organization want to keep that confidential or secret through cloud services with mere hardware requirement and thus remotely accessing all those applications installed on the system of the organization and only selected mac addresses will given the rights to download that file from private cloud and access that file , also referred as “Data security” in the paper.

This approach can drastically minimize the robbery of the confidential data and also with the increasing use of high speed internet; this concept seems more logical and efficient. The application which is used for implementing this concept is of utmost importance because here it’s the application which directly interact with services provided by using private cloud.

Cloud computing refers to the provision of computational resources on demand via a computer network . Users or clients can submit a task, such as word processing, to the service provider, such as Google, without actually possessing the required software or hardware. The consumer's computer may contain very little software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal connected to the Internet. Since the Cloud is the underlying delivery mechanism, Cloud based applications and services may support any type of software application or service in use today .

The essential characteristics of Cloud Computing include On-demand self-service that enables users to consume computing capabilities (e.g., applications, server time, network storage) as and when required. Resource pooling that allows combining computing resources (e.g., hardware, software, processing, network bandwidth) to serve multiple consumers - such resources being dynamically assigned.

Keywords: cloud computing, data security, intruder detection, file sharing, split/merge algorithm ,Deffiehellman algorithm.

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 PURPOSE OF PLAN

The purpose of this project is to overcome the security issues present in a network. The project aims to stop intruder or unauthorised people from accessing a private cloud. Research project address this part as Intrusion Detection. 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).

Currently, if Internet infrastructure assault such as man in the middle attack, denial of service attacks and worms infection, have become one of the most serious threats to the network security It is very likely feasible to detect the attacks and abnormal behaviors if there is sufficient and efficient method and technique exists for monitor and examine, and it can not only make sure proceed warning of potential attacks, but also help out to recognize the reasons, source and locations of the anomalies. By this way, it may assist to restrain the attacks, sooner than they have enough time to broadcast across the network.

This document represents the method, in support of detecting network anomalies by analyzing the unexpected change of accessing of data. With the comparison of other anomaly detection methods. We have focal point on the vibrant behavior of the network rather than using the static models. Our process and method concerns the Auto-Regressive (AR) process to model the rapid and unexpected change of time series data. Our main purpose is to block IP address of a person who is not authorized to access a file and is still trying to do it. It is useful in case of big or small organizations, schools, colleges, business firms, IT firms.

1.2 OBJECTIVE AND PROJECT GOALS

The purpose of this project is to overcome the security issues present in a network. The project aims to stop intruder or unauthorised people from accessing a private cloud. Research project address this part as Intrusion Detection. 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).

The term cloud is analogical to “Internet”. The term cloud computing is based on cloud drawings used in the past to represent telephone networks & later to depict internet in. Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer as a service on pay-as you-use basis. All the info that a digitized system has to offer is provided as a service in the cloud computing model.

Users can access these services available on the “internet cloud” without having any previous know-how on managing the resources involved. Cloud users do not own the physical infrastructure; rather they rent the usage from a third- party provider. They consume resources as a service and pay only for resources that they use. What they only need is a personal computer and internet connection. Cloud computing has revolutionized the IT world with its services provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability. Cloud computing has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications). Hardware layer is not included as it does not directly offer to users. Cloud computing also has three service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates users by providing platform on which applications can be developed and run. IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. SaaS model makes user worry free of installing and running software services on its own machines. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism. IDSs are host-based, network-based and distributed IDSs. Host based IDS (HIDS) monitors specific host machines, network-based IDS (NIDS) identifies intrusions on key network points and distributed IDS (DIDS) operates both on host as well as network. IDSs produce alerts for the administrators which are based on true positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system. IDSs can detect intrusion patterns by critically inspecting the network packets, applying signatures (pre-defined rules) and generating alarms for system administrators. IDS uses two method of detection i.e. anomaly detection, that works on user behavior patterns and suspicious behavior. Other method is misuse detection that can detect through renowned attack patterns and matching a set of defined rules or attack against system vulnerabilities through port scanning.

In general, our aim is to:

- Provide a secure network where intruders can be blocked from accessing the files and data that they are not authorized for.
- To design an executable project which can provide with security and confidentiality to group of people.
- Use two different algorithms namely – Deffiehellman algorithm and split-merge algorithm.
- Using SAAS so that data can be shared among users remotely.

1.3 SCOPE

1.3.1 Scope Definition:

The scope and this project revolves around the security issues present in the network and to overcome them . The project aims to stop intruder or unauthorised people from accessing a private cloud. Research project address this part as Intrusion Detection. 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).
The goal of this project is simple – to provide a necessary protocol specification to allow devices to detect each other when they are in close proximity.

The protocol should satisfy the following objectives –

- Review current intrusion detection system
- Analyze the data with suspicious activities
- Design appropriate system architecture for IDS
- Implement the system using time series analysis
- Testing and evaluate the system.

Other Objectives

- User friendly interface.
- A central database holds the key to system.
- All forms are html templates driven
- Integration among all functional areas.
- The availability of the information is easy.
- Routine tasks are easily performed.
- It automates the redundant tasks.
- It will save time and money.
- In summary, we can say that main objective of the project is to make the work easy and smooth.
- It will provide the better customer service and enhance the profit of the organization.

And we will be making our project by designing's following modules –

Module 1: Password Module

In this module, Employee enters a password and the software checks its validity. If the password is valid then he is allowed to enter, otherwise "Invalid User/Password" message is displayed. Different data access rights are assigned to different users. A new Employee can also be registered in this module.

Module 2: New Client Registration Module

In this module new admin can add details of client machine with IP address and full description.

Module 3 File Sharing Module

In this module admin can share important file to valid client .

Module 4: Intrusion Module

In this module, Admin can share file if invalid user try to hack the file than he can get a file but not valid file. Through this admin can get the IP address of invalid user.

1.4 REQUIRED TOOLS AND SOFTWARES

fig 1.1. Dotnet

DOTNET - The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet. The .NET Framework is designed to fulfill the following objectives:

- To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely.
- To provide a code-execution environment that minimizes software deployment and versioning conflicts.
- To provide a code-execution environment that guarantees safe execution of code, including code created by an unknown or semi-trusted third party.
- To provide a code-execution environment that eliminates the performance problems of scripted or interpreted environments.

- To make the developer experience consistent across widely varying types of applications, such as Windows-based applications and Web-based applications.
- To build all communication on industry standards to ensure that code based on the .NET Framework can integrate with any other code.

The .NET Framework has two main components: the common language runtime and the .NET Framework class library. The common language runtime is the foundation of the .NET Framework. You can think of the runtime as an agent that manages code at execution time, providing core services such as memory management, thread management, and remoting, while also enforcing strict type safety and other forms of code accuracy that ensure security and robustness. In fact, the concept of code management is a fundamental principle of the runtime. Code that targets the runtime is known as managed code, while code that does not target the runtime is known as unmanaged code. The class library, the other main component of the .NET Framework, is a comprehensive, object-oriented collection of reusable types that you can use to develop applications ranging from traditional command-line or graphical user interface (GUI) applications to applications based on the latest innovations provided by ASP.NET, such as Web Forms and XML Web services.
The .NET Framework can be hosted by unmanaged components that load the common language runtime into their processes and initiate the execution of managed code, thereby creating a software environment that can exploit both managed and unmanaged features. The .NET Framework not only provides several runtime hosts, but also supports the development of third-party runtime hosts.
For example, ASP.NET hosts the runtime to provide a scalable, server-side environment for managed code.

Fig 1.2 MYSQL

SQL

SQL is a language for relational database. SQL is a non-procedural i.e., when we use SQL we specify what we want to be done not how to do it.

Features Of SQL

1. SQL is an interactive query language.
2. SQL is a database administration language.
3. SQL is a database programming language.
4. SQL is a client/server language.
5. SQL is a distributed database language.
6. SQL is a database gateway language.

Basic SQL Commands

Data Definition Language commands (DDL)

Data Manipulation Language commands (DML)

Transaction Control Language commands (TCL)

Data control Language commands (DCL)

Data Query Language(DQL)

Fig 1.3 visual studio

VISUAL STUDIO:-

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every level—including adding support for source control systems (like Subversion) and adding new toolsets like editors and visual designers for domain-specific languages or toolsets for other aspects of the software development lifecycle (like the Team Foundation Server client: Team Explorer).

Visual Studio supports different programming languages and allows the code editor and debugger to support (to varying degrees) nearly any programming language, provided a language-specific service exists. Built-in languages include C, C++ and C++/CLI (via Visual C++), VB.NET (via Visual Basic .NET), C# (via Visual C#), F# (as of Visual Studio 2010) and TypeScript (as of Visual Studio 2013 Update 2). Support for other languages such as Python, Ruby, Node.js, and M among others is available via language services installed separately. It also supports XML/XSLT, HTML/XHTML, JavaScript and CSS. Java (and J#) were supported in the past.

CHAPTER 2

LITERATURE REVIEW

2.1 ANALYSIS

In these days a single server handles the multiple requests from the user. Here the server has to process the all requests from the users simultaneously, so the processing time will be high. This may leads to loss of data and packets may be delayed and corrupted. On doing this the server cannot process the query from the user in a proper manner. So the processing time gets increased. It may leads to traffic and congestion. To overcome these problems we are going for the concept called cloud computing. In this cloud computing we are going to implement the proxy server to avoid these problems. But in this system data efficiency is improved but not the data security. Whenever we speak all about data efficiency we should speak about data security also, because in the cloud computing we don't know from which cloud the data is coming, so in the existing system there is no system to find the data security. The system based on the new architecture has better scalability and fault tolerance. A cluster consists of a single server and multiple proxy servers and is accessed by multiple clients. Proxy servers stores data on local disks and read or write data specified by a server. The server maintains the index for all file stored in different proxies. When a client wants to download some data, it will first send a request to the Server and the Server then redirect the request to a corresponding proxy that have the required data and hence the data will be sent to the client. With the combination of Cloud and Grid computing concepts, the data request can be efficiently serviced in a timely manner. The major part of the Project is Security.

Knowledge Analysis: Using an expert system, we can describe a malicious behaviour with a rule. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones. Intrusion detection (ID) is a type of security management system for computers and networks.

2.1RESEARCH RELATED WORK

2.2.1 Intrusion detection using data mining technique:

According to Krishna Kant Tiwari and Sriram Yadav (2012)
Increasing number of public and commercial services are used through the Internet, so that security of information becomes more important issue in the society information Intrusion Detection System (IDS) used against attacks for protected to the Computer networks. On another way, some data mining techniques also contribute to intrusion detection. Some data mining techniques used for intrusion detection can be classified into two classes: misuse intrusion detection and anomaly intrusion detection. Misuse always refers to known attacks and harmful activities that exploit the known sensitivity of the system. Anomaly generally means a generally activity that is able to

indicate an intrusion. Here 23 different research papers were taken together an with the help of big data a graph was picturized based on it.

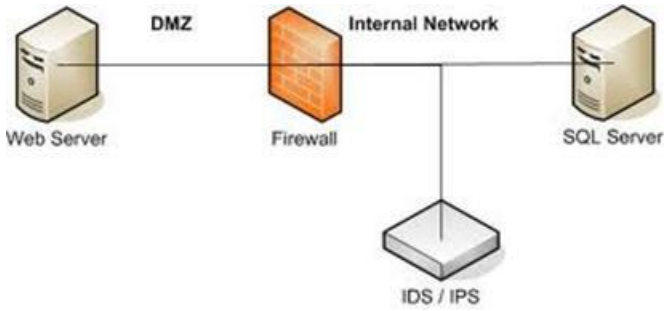

Fig 2.1 IDS system

Intrusion detection using data mining technique detection system plays an important role in the security and perseverance of active defence system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach. In intrusion detection, user data and application is hosted on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS should be the user and not the provider of cloud services. In the paper, Krishna and Sriram have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyses complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.

2.2.2 Intrusion Detection system – a study:

According to Dr. S.Vijayarani and Ms. Maria (2015) research paper -

Types of IDS -

1) Host based IDS

2) Network based IDS

3) Application based IDS

Host based IDS views the sign of intrusion in the local system. For analysis they use host system's logging and other information. Host based handler is referred as sensor. Other sources, from which a host-based sensor can obtain data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms. Host based system trust strongly on audit trail. The information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction. The elementary principle in IDS including Network Based Intrusion Detection System (NIDS) originated from anomaly HIDS research based on Denning's pioneering work. Host-based IDS provides much more relevant information than Network-based IDS. HIDS are used efficiently for analysing the network attacks, for example, it can sometimes tell exactly what the attacker did, which commands he used, what files he opened, rather than just a vague accusation and there is an attempt to execute a dangerous command. It is less risky to configure.

Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

Network based IDS systems collect information from the network itself rather than from each separate host. The NIDS audits the network attacks while packets moving across the network. The network sensors come equipped with attack signatures that are rules on what will constitute an attack and most network-based systems allow advanced users to define their own signatures.
Denial-of-Service (DOS) - Attacks It tries to deny the authorized users from promoting the requested service. An advanced Distributed Denial of Service occurs in a distributed environment that the attacker sends or floods the server with numerous connection that request to knock the target system.

Types of DOS attacks are –

1. SYN Attack -SYN attack is also defined as Synchronization attack. Here, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015 35 3.2.2. Ping of Death In this the intruder sends a ping request to the targeted system which is larger than 65,536 bytes which causes the system to crash. The formal size must be 56 bytes or 84 bytes in case of considering Internet protocol header.

2. Eavesdropping Attacks - It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines or through email.

3. Spoofing Attacks - This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker.

2.2.3 Network and host based attacks on remote Server

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users. Cloud security auditing Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

2.3 Proposed Model

2.3.1 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 centre 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. User requests and actions are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider.

The proposed model is shown in the following figure;

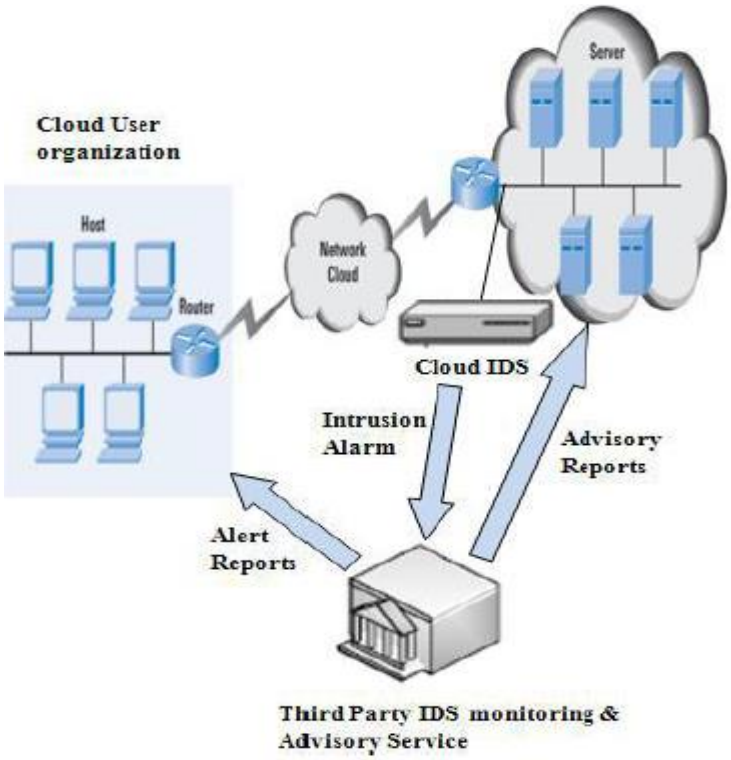

Fig 2.2 Proposed Cloud IDS Model

2.3.2 Advantages of proposed model

1. High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach.

2. CPU, memory consumption as well as packet loss would be reduced to improve the overall efficiency of cloud IDS.

3. In a host based IDS (HIDS) scenario, if host becomes the victim of offending attacker and controlled by the intruder, HIDS on that host would be compromised. In such a case the attacker would not allow HIDS to send alerts to administrator and could play havoc with the data and applications. For better visibility and resistance, network IDS (NIDS) has been proposed for cloud infrastructure.

4. A third party monitoring and advisory service has been proposed, who has both experience and resources to observe/ handle intrusion data and generate reports for cloud user as well as advisory reports for cloud service provider.

5. Being at a central point, proposed Cloud IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach.

2.4 Intrusion Detection System

Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse . It becomes crucial part in the cloud computing environment. The main aim of ids is to detect computer attacks and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network.

There are mainly two categories of IDS, network based and host based. In addition, the ids can be defined as a defence system, which detects hostile activities in a network. The key is to detect and possibly prevent activities that may compromise system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans.

one key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection. Intrusion detection is defined as the process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, ids tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers). Once an intrusion has been detected, IDS issues alerts notifying administrators of this fact. The next step is undertaken either by the administrators or the ids itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization's security policy. An IDS is an element of the security policy. Among various ids tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources.

2.4.1 Host based intrusion detection system (HIDS): this type of ids involves software or agent components, which is run on the server, router, switch or network appliance. However, the agent versions must report to a console or can be run together on the same host as depicted in fig 2.3 Basically, HIDS provides poor real-time response and cannot effectively defend against one-time catastrophic events. In fact, HIDS are much better in detecting and responding to long term attacks such as data thieving .

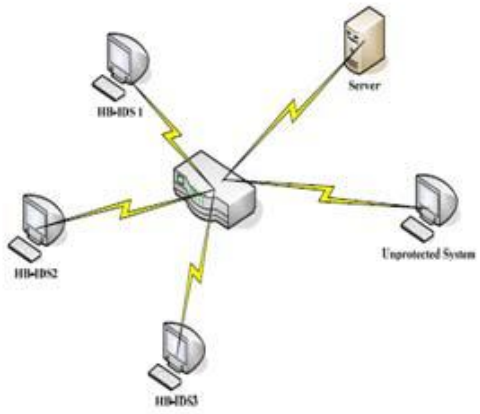

Fig 2.3 HIDS

2.4.2 Network based intrusion detection system(NIDS) : this type of ids captures network traffic packets such as TCP and UDP) and analyses the content against a set of rules or signatures to determine if a possible event took place. False positives are common when an ids system is not configured or "tuned" to the environment traffic it is trying to analyse . Fig 3 shows the network based intrusion detection system.

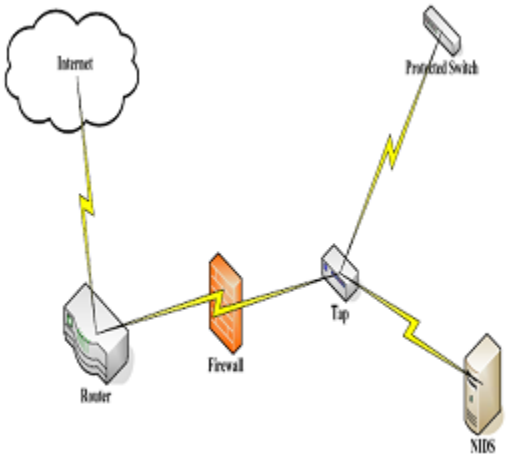

Fig 2.4 NIDS

CHAPTER 3

METHODOLOGY

3.1 Approach to design

Our proposed aim is to build a system that provides efficient and effective security to our LAN network and help us maintaining secrecy and confidentiality of data. The system design mainly focuses on providing security to organization, companies, firms which may be big or small. Firstly, the basic flowchart of the proposed system needs to be drawn and analyzed with full specifications.

3.1.1 Block diagram of proposed system

Context Level DFD

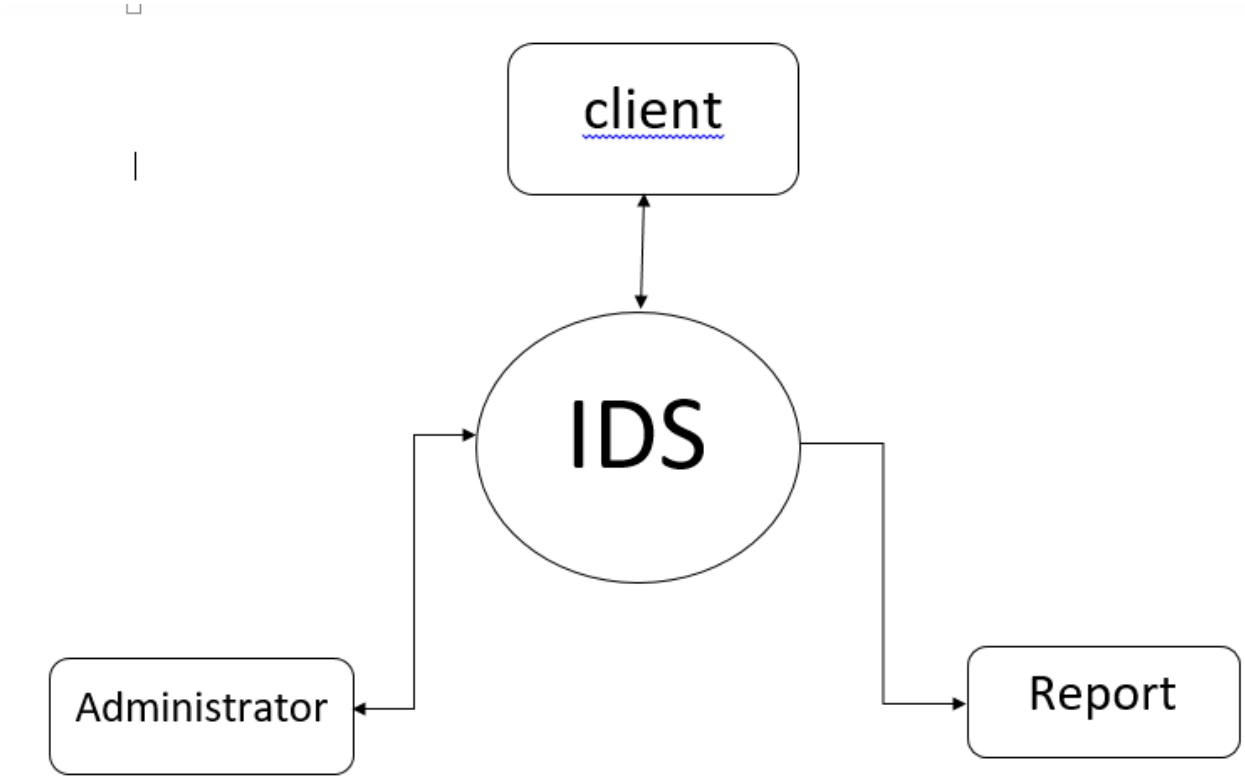

Fig 3.1 context level DFD

Data Flow Diagram (Level-1)

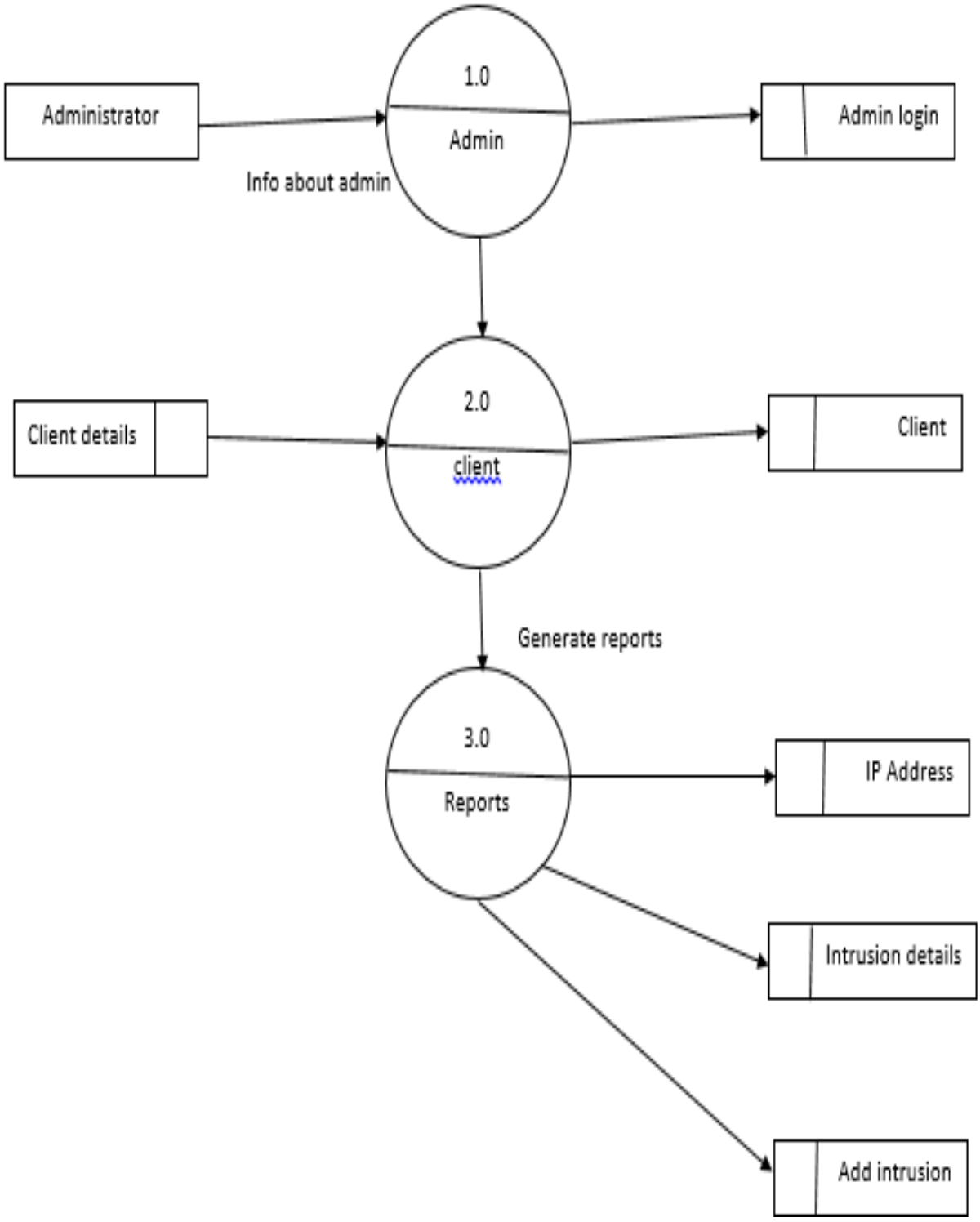

fig 3.2 data flow diagram (level 1)

Second level DFD

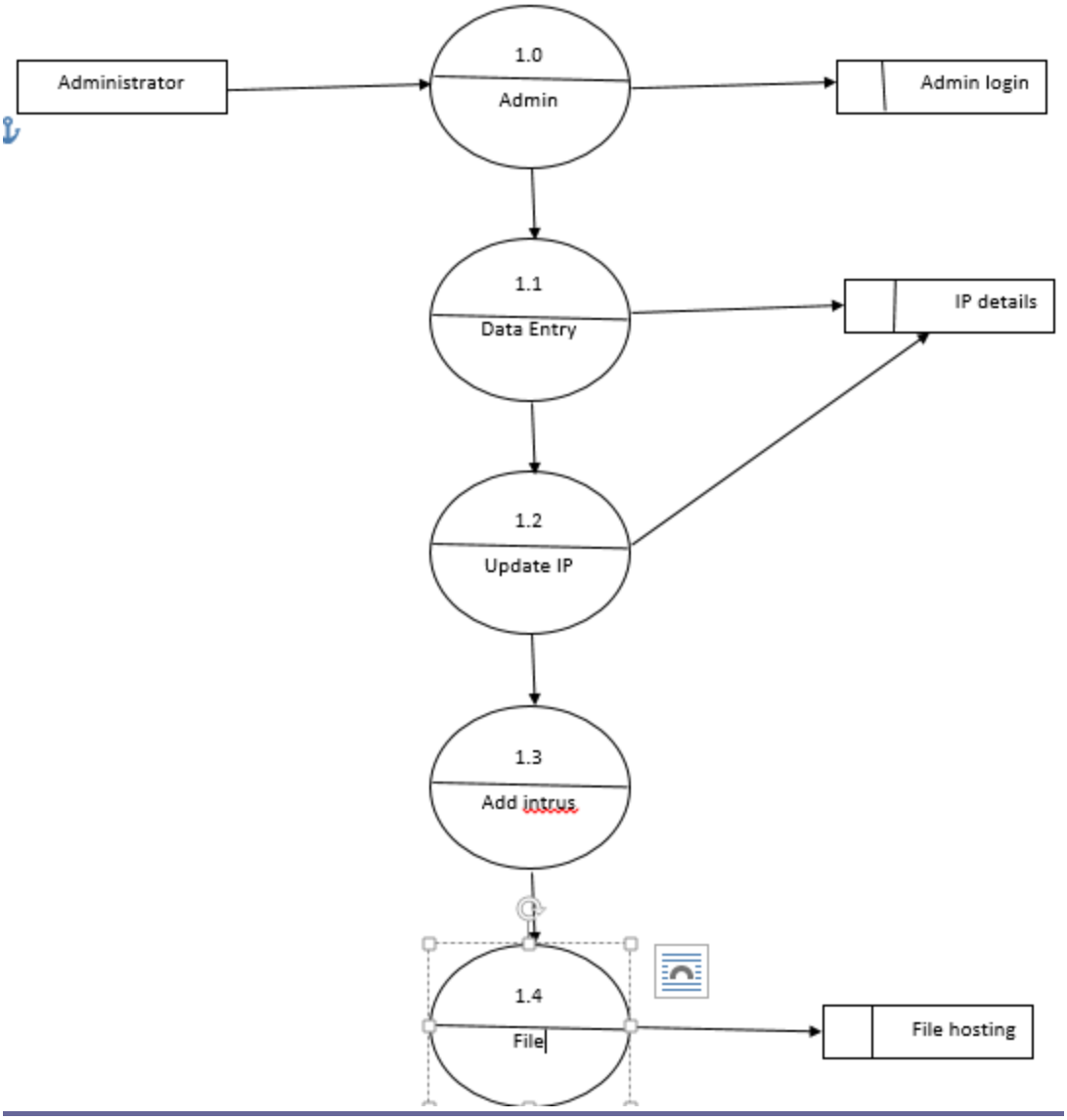

Fig 3.3 DFD level 2

3.1.2 Algorithms used

(a) **Deffie-Hellman algorithm** is a way of generating a shared secret between two people in such a way that the secret can't be seen by observing the communication. That's an important distinction: You're not sharing information during the key exchange, you're creating a key together. This is particularly useful because you can use this technique to create an encryption key with someone, and then start encrypting your traffic with that key. And even if the traffic is recorded and later analyzed, there's absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible. This is where comes from. Nobody analyzing the traffic at a later date can break in because the key was never saved, never transmitted, and never made visible anywhere.
The way it works is reasonably simple. A lot of the math is the same as you see in public key crypto in that is used. And while the discrete logarithm problem is traditionally used (the x^y *mod p* business), the general process can be modified. But even though it uses the same underlying principles as public key cryptography, this is *not* asymmetric cryptography because nothing is ever encrypted or decrypted during the exchange. It is, however, an essential building-block, and was in fact the base upon which asymmetric crypto was later built.
The basic idea works like this:

1. I come up with two prime numbers **g** and **p** and tell you what they are.
2. You then pick a secret number (**a**), but you don't tell anyone. Instead you compute $\mathbf{g}^{\mathbf{a}}$ *mod* **p** and send that result back to me. (We'll call that **A** since it came from **a**).
3. I do the same thing, but we'll call my secret number **b** and the computed number **B**. So I compute $\mathbf{g}^{\mathbf{b}}$ *mod* **p** and send you the result (called "**B**")
4. Now, you take the number I sent you and do the exact same operation with *it*. So that's $\mathbf{B}^{\mathbf{a}}$ *mod***p**.
5. I do the same operation with the result you sent me, so: $\mathbf{A}^{\mathbf{b}}$ *mod* **p**.

(b) **Split and Merge Algorithm** is used to split large files into smaller chunks of your choice and merge them back into single file. This is extremely useful when copying files into floppies or while transferring files over network.
This project consists of a class Split Merge.vb and a user interface to test the class. Source code is provided as a VS.NET project, so you can download the source and build it with current version of VS.NET. I created and tested this under VS.NET with SP2 under Windows 2000.

This project demonstrates the usage of file streams, threading and events in VB.NET
This class has two primary methods SplitFile and MergeFile.

SplitFile
Splits files into smaller chunk files.
FileName: File name to split with full path

OutputPath: Output folder name where the chunk files will be created. Chunk files will be created with the same name as input file with suffix of sequence number (e.g.: bigfile.exe.001)

DeleteFileAfterSplit: Boolean value indicating, whether to delete the input file after splitting.

ChunkSize: Long value indicating the chunk size in bytes.

MergeFile: Merges all the chunk files into one file.

FileName: First chunk file name with full path or the file name with full path

OutputPath: Output folder name where the merged file will be created

DeleteFilesAfterMerge: Boolean value indicating, whether to delete the chunk file after merge.

Both these methods are thread safe and can be called as background threads

Events

This class has 3 events.

FileSplitCompleted - This event is raised after the split process is completed

FileMergeCompleted - This event is raised after the merge process is completed

UpdateProgress - This event is raised to notify the client about the progress. Raised after each chunk file is created.

(c) AES Algorithm for encryption: AES is an iterative rather than Feistel in figure. It relies on upon 'substitution–permutation mastermind'. It contains a movement of associated operations, some of which incorporate supplanting commitments by specific yields (substitutions) and others incorporate reworking bits around (permutations).Interestingly, AES plays out each one of its computations on bytes instead of bits. Subsequently, AES treats the 128 bits of a plaintext upset as 16 bytes. These 16 bytes are composed in four areas and four sections for taking care of as a system − Unlike DES, the amount of rounds in AES is variable and depends on upon the length of the key. AES uses 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256-piece keys. Each of these rounds uses an other 128-piece round key, which is learned from the main AES keytop for report trading: The File Transfer Protocol (FTP) is a standard framework tradition used for the trading of PC records from a server to a client using the Client–server appear on a PC compose.

(d) FTP File Transfer Protocol: is based on a customer server display design and uses isolate control and information associations between the customer and the server.FTP clients may confirm themselves with a reasonable content sign-in convention, ordinarily as a username and secret key, yet can interface namelessly if the server is arranged to permit it. For secure transmission that ensures the username and watchword, and scrambles the substance, FTP is regularly secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is now and again additionally utilized rather, however is innovatively distinctive.

3.1.3. CRM Customer Relationship Management

CRM is a tool which is used Client relationship administration (CRM) is a term that alludes to practices, techniques and innovations that organizations use to oversee and examine client associations and information all through the client lifecycle, with the objective of enhancing business associations with clients, aiding client maintenance and driving deals development. CRM frameworks are intended to gather data on clients crosswise over various stations - or purposes of contact between the client and the organization - which could incorporate the organization's site, phone, live visit, regular postal mail, promoting materials and web-based social networking. CRM frameworks can likewise give client confronting staff itemized data on clients' close to home data, buy history, purchasing inclinations and concerns. It has been used in our project and it is helping us by maintaining the logs of information exchanged between users and also helps in resolving clients/users problems, administrator
has got all the rights to resolve problems that client is facing and this CRM tool make our work very efficient, easy, fast and it is mostly used with cloud services and also for using CRM we should be having internet connection with us.

3.1.4 Pros and Cons of Microsoft visual studio

Visual studio has different points of interest -

•Microsoft's Visual Studio is a develop and rich coordinated advancement condition (IDE). There are three primary forms of Visual Studio IDE: Visual Studio, Visual Studio Code and Visual Studio Online (VSO).

•The objective of every adaptation of Visual Studio is to give rich advancement instruments to all designers all around on any stage. Advancement groups will have the capacity to create programming for Web, portable, server and desktop with Visual Studio.

•Visual Studio IDE gives a rich choice of advancement dialects. At present, designers can create applications with Visual Basic, C#, PHP, Objective-C, JavaScript and Visual C++. The API establishment for Microsoft improvement is known as the .NET Framework, and offers help for dialect interoperability.

There are similarly various obstacles. They are:

•Weak Documentation: Visual studio(C++) documentation is bad. Be that as it may, the python documentation is surprisingly more terrible. A fledgling client is left think about how to utilize certain capacities. There are less instructional exercises for Visual studio (Python).

•Lack of bolster: Companies that bolster Visual studio (Intel, AMD, NVidia and so on) have a puppy in the battle with regards to the C++ rendition of Visual studio. They need you to utilize Visual studio and to purchase their equipment (CPUs/GPUs and so on.) to run these calculations. In any case, Visual studio (Python) is by all accounts the famous red-headed stride tyke that does not appear to stand out enough to be noticed.

•Slower run time : Compared to C++, programs in Python will regularly run slower. To include an additional punch you can utilize the GPU (utilizing CUDA or OpenCL) in Visual studio (C++) and have code that runs 10x speedier than the Python usage.

•Visual studio is composed in C/C++ : One of the immense advantages of an open source library is your capacity to alter them to suit your necessities. On the off chance that you need to alter Visual studio, you need to adjust the C/C++ source.

Intruder detection system prevents any intruder from entering our LAN network intruder is a person who is not authorized who have no right to access the file which can be done as follows: -

- Welcome page to the application here user have 2 choices by which he/she get the right to enter the application for sharing the secret file i.e., either login or register as shown below in figure.

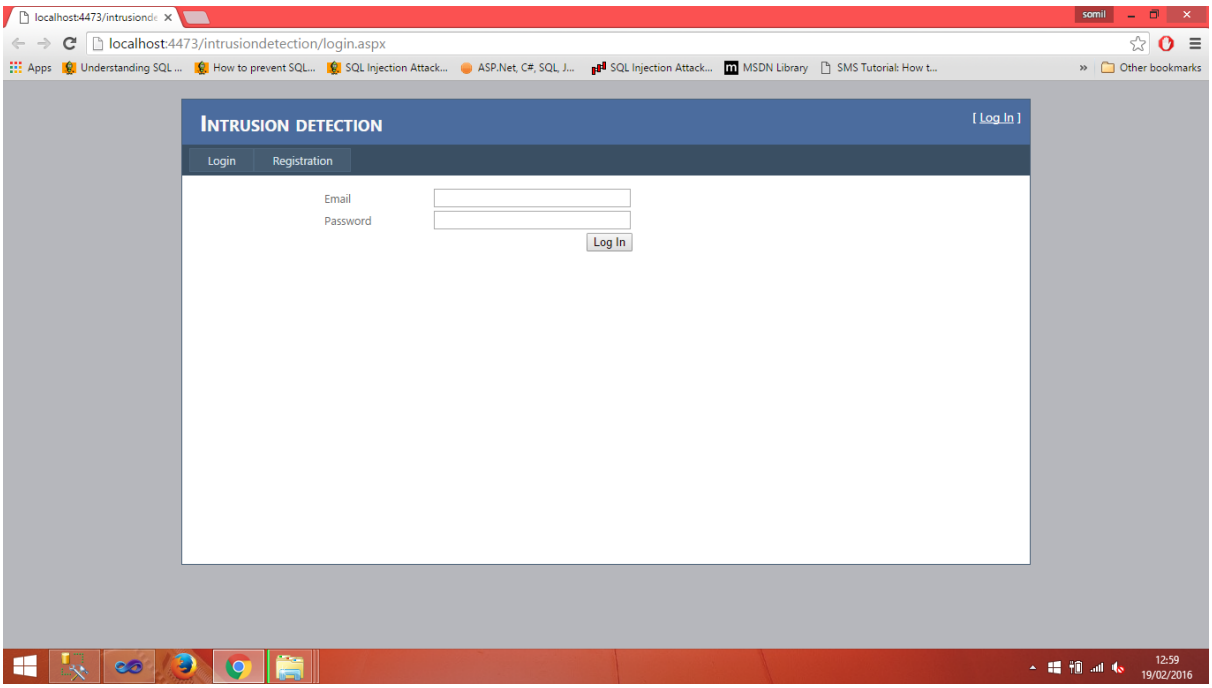

Fig 3.4 welcome page

- If user go for register he/she have to fill up the form as shown below in the figure here our application fetches the IP Address and Mac address of the system/device which the user is using while filling up the form.

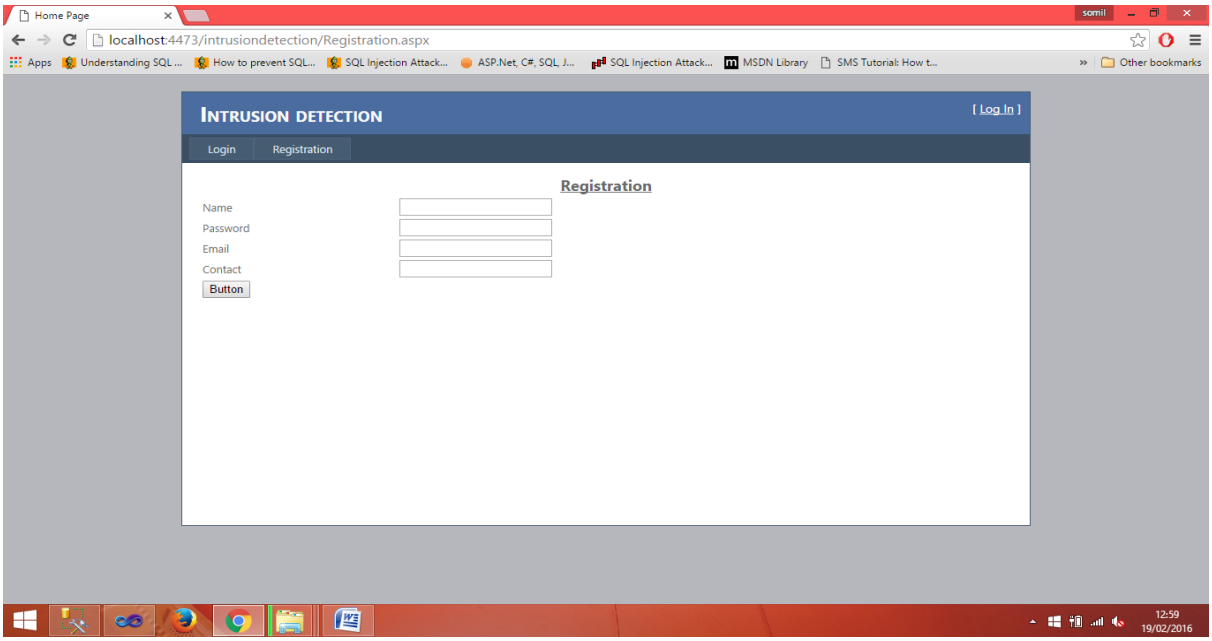

Fig 3.5 registration window

- Now after the registration its on admin to approve the user to get the rights to that file sharing LAN network or not if admin allows from the approve user window.
- After approval of the registration the user gets the right to enter the LAN network now he/she can go to the split-n-join window for splitting file into parts as many as he/she wants to do as shown below in figure.
- First method of sharing the parts of the file here user have to the form.
- The user who want to access the whole document user have to go to the split-n-join window for joining the parts of the file and then he/she can download and access the whole document.
- Second method of sharing the file user can use encrypt/decrypt window

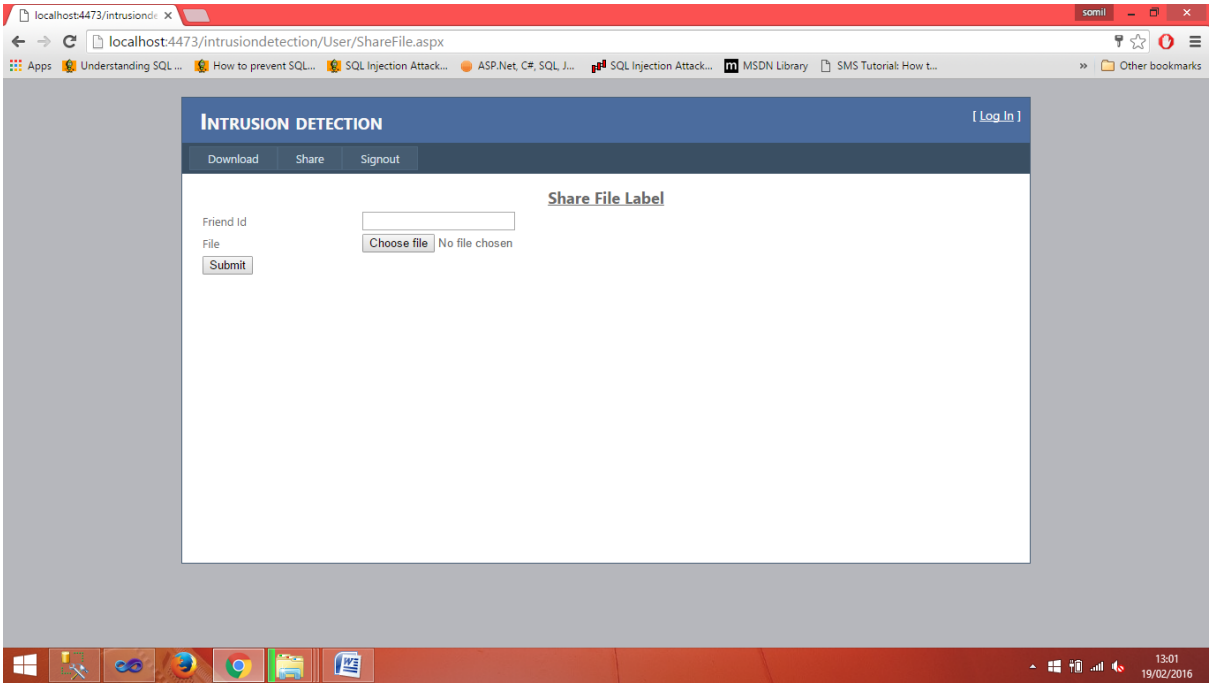

Fig 3.6 file sharing window

- If any unauthorized person/intruder will try to enter the network than his/her mac address and IP address will be fetched and user will be blocked to access the LAN and his/her details will displayed at the view intruder window of the admin panel.

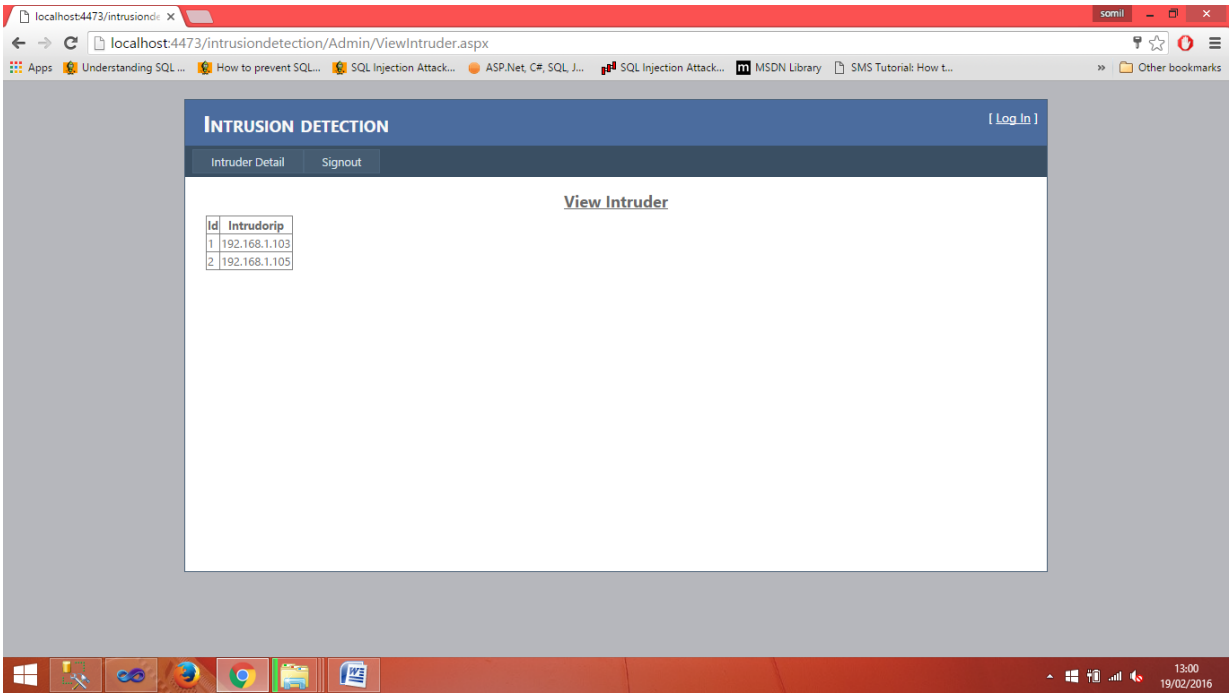

Fig 3.7 intruder details window

- Admin can also check which files are shared at which time by which IP address mac address.
- In case if intruder get the file access he/she will get the access to the part only he/she cannot merge the parts of the document because as we used deffie-hellman algorithm here intruder do not have the secret key which was generated at the time of file sharing.

3.2 Tools and Technologies used

Microsoft Visual Studio is a coordinated advancement condition (IDE) from Microsoft. It is utilized to create PC programs for Microsoft Windows, and in addition sites, web applications, web administrations and portable applications. Visual Studio utilizes Microsoft programming advancement stages, for example, Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can create both local code and oversaw code.
Visual Studio incorporates a code editorial manager supporting IntelliSense (the code fulfillment part) and in addition code refactoring. The coordinated debugger works both as a source-level debugger and a machine-level debugger. Other inherent apparatuses incorporate a code profiler, shapes originator for building GUI applications, website specialist, class fashioner, and database composition creator. It acknowledges modules that improve the usefulness at practically every level—including support for source control frameworks (like Subversion) and including new toolsets like editors and visual planners for area particular dialects or toolsets for different parts of the product advancement lifecycle (like the Team Foundation Server customer: Team Explorer).

Visual Studio bolsters diverse programming dialects and permits the code manager and debugger to support (to shifting degrees) almost any programming dialect, gave a dialect particular administration exists. Worked in dialects incorporate C, Java, VB.NET (through Visual Basic .NET), C#.

3.3 Hardware Requirements

Working System: Windows 10/8.1/8/7

Processors : Any Intel 64-x86 processor

Smash : 2 GB is suggested

Plate Space: 5-6 GB for typical installation a run of the mill establishment, 5 GB for VISUAL STUDIO

CHAPTER 4

RESULT

RESULTS AND DISCUSSIONS

Cloud computing is a “network of networks” over the internet, therefore chances of intrusion is more with the erudition of intruder’s attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this report, a multi-threaded cloud IDS model is proposed which can be administered by a third-party monitoring service for a better optimized efficiency and transparency for the cloud user.

This software will help the admin to make his job easier and also help the company to make its network more safe, secure and protect form unauthorized people who try to access data that is not meant for them and snoop around with confidential details making it difficult for companies, organizations to protect their data. Here if an intruder tries to enter the system then a mail will be sent to the admin which will notify him about some malicious activity and there will be IP address of that intruder which the admin will be able to see, if the intruder tries to download some file form the private cloud that is only for a particular group of people then with the help of split/merge algorithm he will be able to download a part of a whole file or it can also be a random file which will be of no use to the intruder and simultaneously the admin have the rights to block that particular IP address form accessing the private cloud again in future.

Security measures that will be present in our system will be – there will be password verification with user name matching, there will be text matching of messages that will be exchanged within a private cloud and an alarm notification will be sent via email to admin if an intruder tries to access the private information of a company or organization.

SECURITY AGAINST UNAUTHORIZED ACCESS:

- Use of administrator passwords: The password provides security to the administrator of Associates user so that unauthorized user cannot access the facility of Associates User.
- User related checks and validations: For this software, the developer uses user related checks and validations from the user.

SECURITY AGAINST DATA LOSS:

- Provision of efficient data backup system : In this software an efficient system is used for adequate backup facility .
- Offline data storage : this system is capable for offline data Storage.
- Multiple database backup: the efficient system is use for this Software to give multiple data backup.

Intruder details

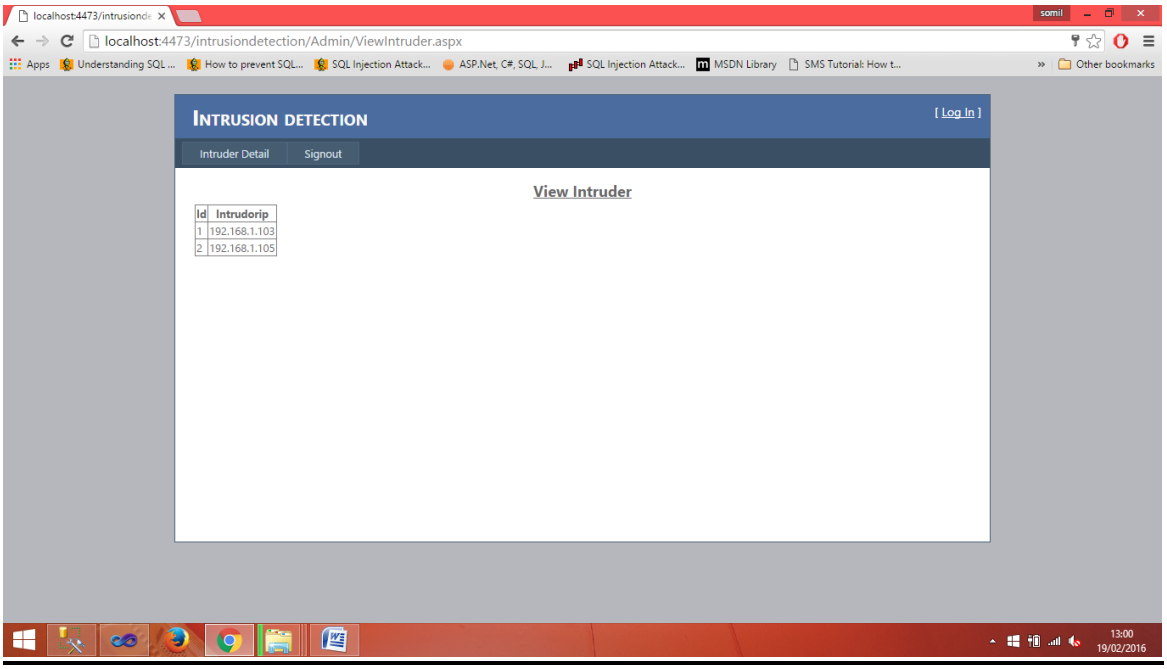

Fig 4.1 intruder details

GANTT CHART OF THE ACTIVITY

A Gantt chart is a type of bar chart, developed by Henry Gantt, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Some Gantt charts also show the dependency (i.e., precedence network) relationships between activities.

Gantt charts are useful tools for planning and scheduling projects.

- Gantt charts allow you to assess how long a project should take.
- Gantt charts lay out the order in which tasks need to be carried out.
- Gantt charts help manage the dependencies between tasks.
- Gantt charts determine the resources needed.
- Gantt charts are useful tools when a project is under way.
- Gantt charts monitor progress. You can immediately see what should have been achieved at a point in time.
- Gantt charts allow you to see how remedial action may bring the project back on course.

TASKS	Dec 1'st &2'nd Week	Dec 3'rd & 4'th Week	Jan 1'st & 2'nd Week	Jan 3'rd-Jan 4-th Week	Feb 2'nd & Feb 3'rd Week	Feb 4'rd & Mar 1'st Week	March2'st & Mar 3'rd Week	Apr 1'st & 2'th Week	Apr 3'rd Week
Problem Analysis	Day 1-12 12 Days								
Analysis of Existing Systems like the proposed on		Day 13-22 10 Days							
Selection & Learning the S/W To be used			Days 23-32 10 Days						
Understanding Techniques and algorithm				Days 33-47 15 Days					
Trying practical implementation					Days 48-62 15 days				
Designing						Days 63-72 10 days			
Testing							Days 73-82 10 Days		
Evaluation								Days -83-92 10 Days	

Implementation									Days 93-986 Days

CHAPTER 5

CONCLUSION & FUTURE PROSPECTS

While writing this project, I and my partner have been besieged by the nature and amount of information available to us from the internet today. We have assiduously have been working with our mentor, Deepak Gaur sir, and our esteemed program leader, Kunal Gupta sir, both of whom have made this significantly easier to do. Our project was and still is one of the ground-breaking thoughts in our batch and we are very happy to have worked on it as we have. As mentioned earlier, This is a completely research based project and we are very happy to have worked on it as we have, this is a completely research based project and thus, for the sake of development modest assumptions will be taken into contemplation every step of the way. Firm assumptions could be made as intruder was detected if he does not match the group of IP and Mac addresses allowed to access the data or files. This approach of our will help us in securing our files, data and maintaining security and integrity of the system. The outcome of this project will be delivered on the software called visual studio and we will be successful in our aim only if we are able to block the IP address of the intruder who is not allowed to the gain the access of the file and prevent him from entering our private cloud and LAN network too. Today the security plays a very crucial role for each company weather it is big or small, universities, offices, schools, government, personal day to day communication. so this project will further help us in strengthening the security issues and make people less worried about any kind of breach into their confidential matters. Our final result has been very special then we anticipated. Our project will help new avoiding new upcoming threats and will act as a milestone in the science fields. Here we will be using two algorithms for the first time namely split/merge algorithm and deffie-hellman algorithm.
We are trying to make our project more efficient and robust.

The IDS is for the manage process can be further developed into a separate, automated system with the following enhancements:

• Help file can be included. The system, as of now, does not support any help facility for the users of the system. A help menu can be provided with a special function key and help command in the main page itself. Help can be either introduced as a separate window, a reference to a printed manual or as one or two line suggestion produced in a fixed screen location.

• The system can use typed commands, as they were once the most common mode of communication with the system. The typed command can be provided through control sequence or function keys or typed word.

• A training module can be included in the system. This module can be used to train the users of the system about the systems usage.

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] J. Mchugh, A. Christie, and J. Allen, “Defending Yourself: The Role of Intrusion Detection Systems”, IEEE Software, Volume 17, Issue 5, Sep.-Oct., pp. 42-51, 2000.

[8] K. V. S. N. R. Rao, A. Pal, and M. R. Patra, “A Service Oriented Architectural Design for Building Intrusion Detection Systems”, International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 11-14, 2009.

[9] Information Technology at Johns Hopkins-Glossary G-I, http://www.it.jhmi.edu/glossary/ghi.html

[10] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes