ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1868-1873

INTRUSION DETECTION SYSTEM FOR CLOUD SYSTEM USING INTELLIGENT AGENTS

Manikandaprabu.M, Karthi.M[#], Shanmugapriya.R[#], Sultan.M[#], Ameela.T[#], Muruganandham.N[#]

***Abstract*—Cloud computing allows the end users to use the application without installation and access their personal files at any computer with internet access. Apart from the advantages of cloud environment, security is the major issue. Due to the distributed nature, cloud environment is an easy target for intruders looking for the possible attacks to exploit. To address the security issues in the cloud environment an Intrusion Detection System (IDS) is proposed based on the features of the mobile agent. The mobile agents are used to collect and analyze the data collected from cloud environment to identify attacks exploited by the intruders. The main objective of the proposed system is to detect the known and unknown attacks exploited by the intruders in the cloud environment.**

***Keywords*-- Cloud computing, Intrusion Detection System, Mobile agent, intruders.**

I. INTRODUCTION

Cloud computing means a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the service provider and consumer. In cloud environment the systems are distributed so there is greater chance of exploiting attacks by the intruders. The intruders are the one who uses the services without any authorization and misuses the privileges. The intrusion detection means the process of detecting the individual who misuses the privileges assigned to them and one who access the data or service of legitimate user without any authorization. The intrusion detection system was designed to detect the intruders trying to exploit attacks in the network. In this proposed system the intrusion detection system uses the mobile agent to detect the attacks being exploited by the intruders.

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. The goal of IDS is to detect suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat.

An attack against a cloud computing system can be silent for network-based IDS deployed in its environment, because node communication is usually encrypted. Attacks can also be invisible to host-based IDS, because cloud-specific attacks don't necessarily leave traces in nodes operating system, where the host –based IDS resides. In this way, traditional IDS can't appropriately identify suspicious attacks in cloud environment.

The mobile agent is an agent having the capability of moving from one host to another. It interacts with the other nodes to collect the data. The advantage of mobile agent technology are reduces the network overload, overcoming network latency, robust and fault tolerant and it works in heterogeneous environment. The mobile agent technology has been shown to be very suitable to solve intrusion detection in a distributed environment. The proposed system employs the mobile agent technology to detect the known and unknown attacks exploited by the attacker.

In addition, cracking technology has evolved into complex approach such as coordinated attack and cooperative attack. Under these circumstances, there is a great need for software tools that can automatically detect a variety of intrusions. As an important gatekeeper of network, *Intrusion Detection Systems* (IDS) must have the ability to detect and defend intrusions more proactively in shorter period.

Basically, two intrusion detection strategies can be distinguished: *anomaly detection* and *misuse detection*. Anomaly detection systems monitor the system and try to decide whether its behavior is normal or not. This is achieved by keeping a normal user profiles. To detect abnormal activity, the predefined profiles are compared with the actual ones in use. The deviation will activate an alarm. In fact, the anomaly detection techniques can be effective against unknown or novel attacks since no prior knowledge about specific intrusion is required. However, they tend to generate more false alarms because an anomaly can just be a new behavior. Otherwise, misuse detection systems search for known *attack signatures*. A signature is a trail of a known attack. For example, it may be a specific series of bits in the header of an

IP packet. A weakness of these systems is that they are not effective against novel attacks that have no matched signatures. In addition, once a new attack is discovered and its signature developed, often there is a substantial latency in its deployment.

As accuracy is the essential requirement for an IDS, its extensibility and adaptability are also critical in todays

network computing environment. However, current IDS have some shortcomings as follows:

- Most IDS detect attacks by analyzing information from a single host, or a single network interface, at many locations throughout the network. Consequently, IDS components miss the communication and the cooperation between each other. This fact hampers the capability to detect large-scale distributed attacks.
- Most commercial IDS are built in hierarchical architecture, which is a tree structure with a control system at the top, information aggregation units at the internal nodes,and sensor units at the leaf nodes. In this kind of system, large amount of data transferred across the network may result in network congestion.
- Because of the reliance on hierarchical structures, many IDS are susceptible to be attacked. An attacker can cut off a control branch of the IDS by attacking an internal node or even decapitate the entire IDS. Typically, such critical components have been hardened to resist direct attacks. Nevertheless, other survivability techniques such as redundancy, mobility, dynamic recovery etc, are showed to be missing in current IDS.
- Many IDS cannot adequately combine history intrusive alarms to analyze future intrusive behaviors. "*Knocking attack*" is an illustrative example. It means that many IDS have no ability to dynamically adjust detective policy by the former intrusive results.

II. Related Work

The IDS should protect the system and needed to be able to resist attack and also needed to be fault tolerant, highly adaptable and configurable. According to the above characteristics, the agent technology is appropriate alternative to develop intrusion detection system. The mobile agent based intrusion detection system were developed which uses the trace gray technique to detect the intrusions. A proposed efficient anomaly intrusion detection system in Ad-hoc by mobile agents which uses the data mining algorithm to detect the attacks exploited by the intruders. Mobile agent based intrusion detection system for MANET proposed by yinan Li which uses the clustering and joint detection technique to identify the intruders. Imen Brahmi proposed in a distributed mobile agent based intrusion detection system, called MAD-IDS. The architecture of the MAD-IDS is based on detection of known and unknown attacks which uses the clustering and rule mining technique. Intelligent intrusion detection system framework using mobile agents which detects the intruders based on the user profile and process profile. Research on distributed intrusion detection system based on mobile agent who increases the system flexibility and security. Signature based method is used in distributed intrusion detection using mobile agents against DDoS attacks. It is proposed a distributed intrusion detection using aglet mobile agent technology which uses the anomaly detection method. Trust modeling technique is used in agent based network intrusion detection system which detects the intruders based on the trust established between the systems. It is also proposed by a intrusion detection system based on agents which uses the STAT technique to detect the attacks.

The main thrust of this paper is to propose new distributed IDS, called **MAD-IDS** (*Mobile Agent using Data mining based Intrusion Detection System*). The MAD-IDS system integrates the data mining algorithms and the mobile agent technology, whose objectives are:

- Improving the distributed IDS performance.
- Detection of both known and unknown attacks with a high accuracy in a distributed environment.
- Reduction of false alarms.

Overview of IDS And Mobile agent

The scalability problem of cPIR is focused in the proposed method, which involves designing a Distributed DB Architecture with peers for processing cPIR Queries.

A. Intrusion detection system (IDS)

Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized Entrance, activity, or file modification.

There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic;
- Identifying abnormal activities;
- Assessing severity and raising alarm.

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- Sensors which generate security events;
- Console to monitor events and alerts and control the sensors;
- Central Engine that records events logged by sensors in a database and uses a system of rules to generate alerts from security events received.

IDS tools aim to detect computer attacks and computer misuse, and to alert the proper individuals upon detection. IDSs use policies to define certain events that, if detected will issue an alert. Certain IDS have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many IDSs not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. IDS are an integral and necessary element of a complete information security infrastructure performing as "the logical complement to network firewalls".

B. IDS techniques

There are four basic techniques used to detect intruders:

- Anomaly detection
- Misuse detection (signature detection)
- Target monitoring

- Stealth probes

C. MOBILE AGENT

The software agent can be treated as Mobile agent [8], as they are able to migrate from one computer to another computer. The mobile agents are very powerful programs, which can act even in the absence of the machine that initiated them. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate. Useful Characteristic of Mobile agents are

- Autonomy: Agents are independently running entities, they operate without human control.
- Mobility: Agents are able to suspend processing on one platform and to move to another one where they resume execution.
- Rationality: Agents embody the capacity to analyze and solve a problem in a rational manner.
- Reactivity: Agents perceive their environment and adapt their behaviour in a dynamic way to match, as soon as possible, new environment parameters.
- Inferential capability: Agents are able to share a set of knowledge in order to achieve a specific goal.
- Pro-activeness: Agents can decide to adapt their behaviour to their environment,
- Social ability: Agents are able to meet and interact with other agents. The interaction and collaboration between agents is achieved by an Agent Communication Language (ACL) and it may depend on ontology.

D. ADVANTAGES OF USING MOBILE AGENTS

The advantages of using mobile agents in IDS are listed below:

- Minimizing the network traffic
- Structure and Platform independence
- Dynamic nature
- Operates in heterogeneous environment
- Robust
- Fault tolerant
- Overcomes network latency
- Scalable.

III. PROPOSED WORK

A. SYSTEM ARCHITECTURE

The Intrusion detection system for cloud is proposed based on the mobile agent, which uses the data mining technique to detect the intrusions in the cloud environment. It contains various mobile agents for collecting and analyzing the data in the cloud environment. There are different agents used to detect the intrusions, they are as follows, Collector agent, Misuse detection agent, Anomaly detection agent, Classifier agent and alert agent.

These agents are used to collect and analyze the data collected from cloud environment to detect the attacks exploited by the intruders.

B. SYSTEM DESCRIPTION

1. COLLECTOR AGENT:

The collector agent is the first agent to work in the system, since it connects to the network. It collects the data from the cloud environment and stores those data in the file. This file is given as an input to the misuse detection agent.

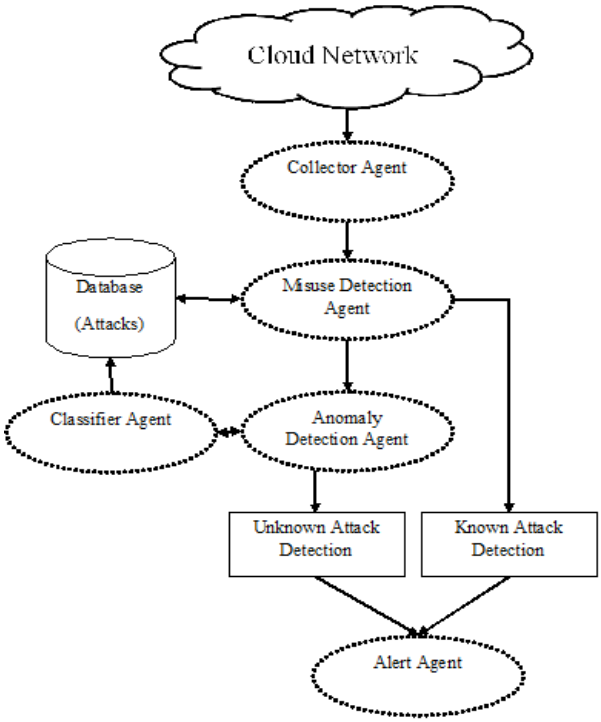

Figure1. System Architecture

2. MISUSE DETECTION AGENT:

The misuse detection agent is used to analyze the data captured by the collector agent. It detects the known attacks in network by using the pattern matching algorithm. If there is a similarity between the collected packets and attack signatures in the database, then it reports to alert agent.

3. ANOMALY DETECTION AGENT:

The anomaly detection agent is used to detect the new or unknown attacks by using the classification techniques. The anomaly detection agent collects the data from the misuse detection agent to analyze the data to detect the unknown attacks, it feds the data to classifier agent to detect the new attack.

4. CLASSIFIER AGENT:

The classifier agent uses the naïve bayes classifier to detect the new attack. It classifies the data based on the dataset available in the database. If the incoming data is detected as attack means then it reports to anomaly agent, which in turn reports to alert agent about the attack. It updates the detected attack in the database.

5. ALERT AGENT:

The alert agent is used to alert the system if any intrusion occurs in the network. It alerts the system based on the output of the misuse and anomaly detection agent.

IV. IMPLEMENTATION

JADE (Java Agent Development framework) is a software framework which is used to implement the mobile agents for the proposed intrusion detection system. The collector agent is assigned a task to collect the data from the cloud environment and stores it as a file. The file is then forwarded to the misuse detection agent, it analyses the data by matching the collected data with the attacks available in the database, and if the data is similar to the patterns in the database then it reports to alert agent. If the data is not matched with the database then the classifier agent is used to classify the data based on the dataset and then it reports to alert agent and updates the database about the attack. The alert agent alerts the system based on the outcome of misuse and anomaly detection agent.

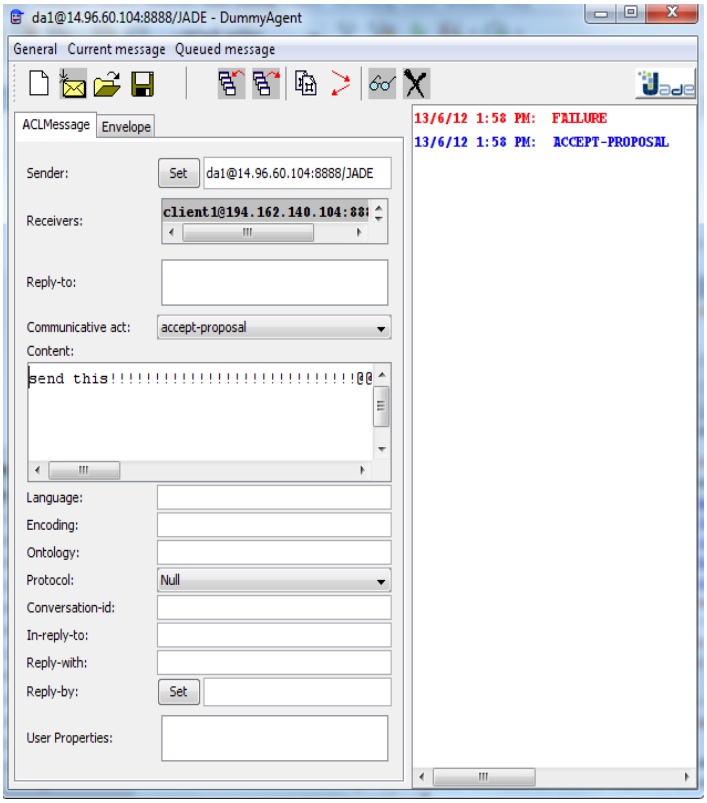

Figure2. Message Forwarding User

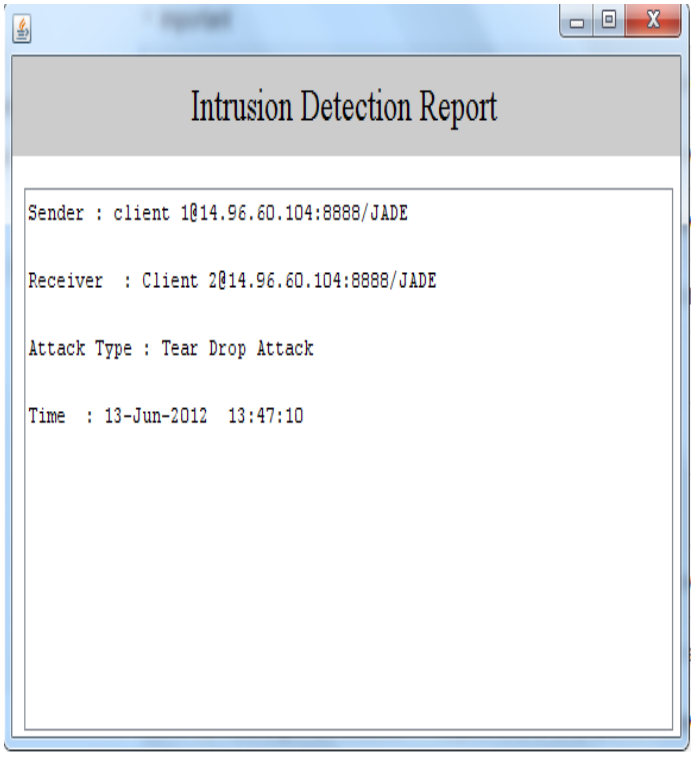

Figure3. Intrusion Detection Report

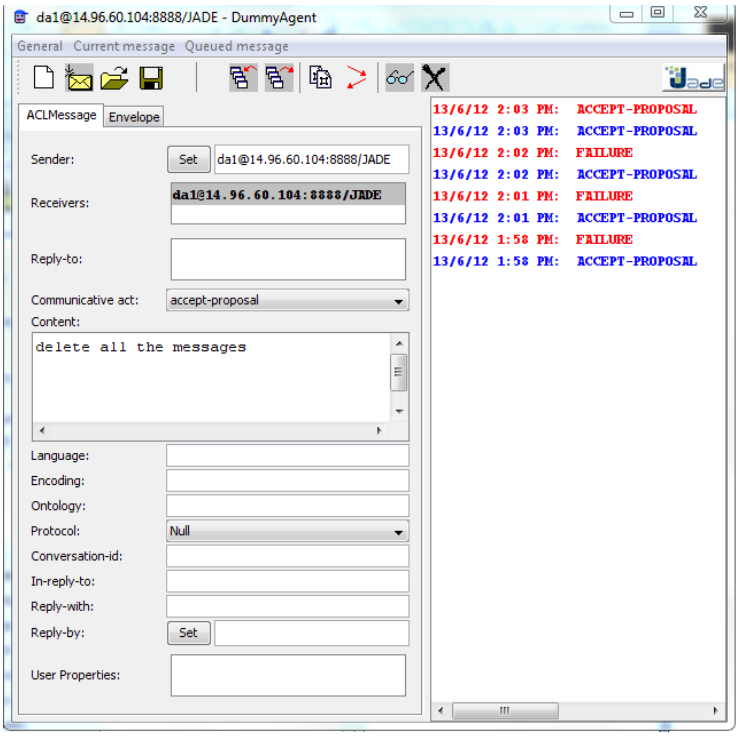

Figure4. Message Forwarding Agent

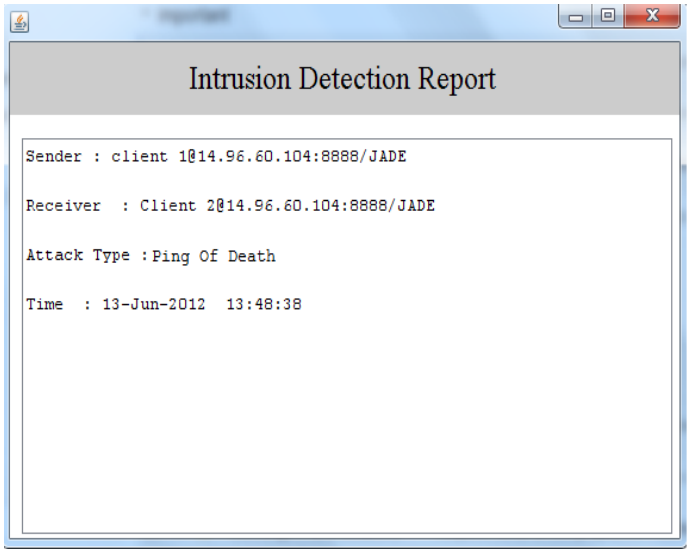

Figure5. Intrusion Detection Agent

V. CONCLUSION

The IDS for cloud computing is proposed which integrates the mobile agent and the data mining technique to detect known and unknown attacks. All the mobile agents are configured in order to perform the operations like collecting the data from cloud environment, and these data are analyzed by the misuse detection agent. This agent checks whether the data collected are matching with the attack dataset available in the database. If any collected data is matched then the misuse detection agent informs the alert agent to alert the system about the intrusion. On the other hand, if the collected data is not matched with the dataset then the collected data are analyzed by anomaly detection agent, which uses naïve bayes classifier to detect the unknown or new attacks. The final result will be such that the known and unknown or new attacks are detected by the proposed architecture.

REFERENCES

[1] Imen Brahmi, Sadok Ben Yahia, and Pascal Poncelete, "MAD-IDS: Novel Intrusion Detection System using Mobile Agents and Data Mining approaches" in Intelligence and Security Informatics, Pacific Asia Workshop, PAISI 2010, Vol 6122, pp:73-76, June 2010.

[2] Ani Taggu, Amar Taggu, "TraceGray: An Application layer scheme for intrusion detection in MANET using Mobile agents" in Third International Conference on Communication Systems and Networks, pp: 1-4, January 2011.

[3] Esfandi. A, "Efficient anomaly intrusion detection system in Ad-hoc networks by Mobile Agents" Third IEEE International Conference on Computer Science and Information Technology, Vol 7, pp:73-77, July 2010.

[4] Yinan Li, Zhihong Qian, "Mobile agents based intrusion detection system for mobile Ad-hoc network" in International Conference on Innovative Computing and Communication, pp: 145-148, March 2010.

[5] N.Jaisankar, R. Saravanan, K. Duraisamy, "Intelligent intrusion detection system framework using mobile agents" in International Journal of Network Security and its Applications, Vol 1, No 2, July 2009.

[6] Jin-Gang-Cao, Gu-Ping-Zheng, "Research on distributed intrusion detection system based on mobile agents" in Seventh International Conference on Machine Learning and Cybermatics, Vol 3, pp: 1394-1399, July 2008.

[7] Ugur Akyazi, A. Sima Etaner Uyar, "Distributed Intrusion detection using mobile agents against DDoS attacks" in 23rd International Symposium on Computer and Information Sciences, pp: 1-6, October 2008.

[8] Manmeet Singh, S.S Sodhi, "Distributed intrusion Detection using Aglet Mobile agent technology" in Proceedings of National Conference and Opportunities in Information Technology (COIT), pp: 148-153, March 2007.

[9] Vojtech Krmicek, Pavel Celeda, Martin Rehak, Michael Pechoucek, "Agent based network intrusion detection system" in International Conference on Intelligent Agent Technology, pp: 528-531, August 2007.

[10] Bin-Dong, Xiu-Ling-Liu, "An improved intrusion detection system based on agents" in Sixth International Conference on Machine Learning and Cybermatics, Vol 6, August 2007.

[11] W. A. Jansen, "Intrusion Detection with Mobile Agents", in Computer communication, Vol: 15, pp: 1392-1401, July 2002.

[12] Mell P, Karygiannis T, W. Jansen, "Mobile Agents in Intrusion Detection and Response", in proceedings of the 12th annual Canadian Information Technology Security Symposium, pp: 1-12, June 2000.

BIOGRAPHY

M.ManikandaPrabhu is currently a PG Scholar in the Department of Computer Science and Engineering at St.Michael College of Engineering and Technology, Sivagangai. He received his Bachelor Degree in Computer Science and Engineering from P.T.R College of Engineering and Technology, Madurai, in 2009. His Research areas include cloud computing, distributed system and network Security.

M.Karthi is currently a PG scholar in Department of Computer Science and Engineering at Velammal College of Engineering and Technology, Madurai. He received his Bachelor Degree in Information Technology and Communication Engineering from Sri Sowdambika College of Engineering, Virdhunagar District, Aruppukottai, in 2009. His Research areas include data mining and data warehousing, cloud computing and distributed system.

R.Shanmuga Priya is currently PG Scholar in Computer Science and Engineering from the Anna University Madurai and she received the B.Tech degree in Information Technology from Anna University Chennai, TamilNadu in 2009. His research areas include cloud computing, Data mining and distributed computing.

M.Sultan is currently a PG scholar in Department of Computer Science and Engineering at St.Michael College of Engineering and Technology, Kalayarkoil, Sivagangai. He received his Bachelor Degree in Information Technology and Communication Engineering from K.L.N.College of Information Technology, Sivagangai, in 2009. His Research areas

include, grid computing, cloud computing and wireless sensor network security

T.Ameela is currently a PG scholar in the Department of Computer Science and Engineering at St.Michael College of Engineering and Technology, Kalayarkoil, Sivagangai. She received her Bachelor Degree in Information Technology from Sakthi Engineering College, Chennai, in 2011. Her research interests include data mining and data warehousing, Semantic web and Network Security

N.Muruganandham is currently a PG Scholar in the Department of Computer Science and Engineering at St.Michael College of Engineering and Technology, Sivagangai. He received his Bachelor degree in Computer Science and Engineering from Shanmuganathan Engineering College, Pudukottai, in 2010. His Research areas include cloud computing, grid computing, and wireless sensor network security.