CHAPTER 4

4. INTRUSION DETECTION SYSTEM FOR THREAT IDENTIFICATION OF INTERNET OF THINGS USING ANSVN

The Internet of things (IoT) is still in its infancy and it is going to be used in many fields in future. The IoT requires strong security solutions where the communication is secured with confidentiality, integrity, and authentication services; the network is protected against intrusions and disruptions. The IoT network is secured with encryption and authentication, but it cannot be protected against cyber-attacks. So it is proposed the ANSVN Algorithm to protect IoT networks from intrusions.

4.1 INTRODUCTION

The Internet of Things (IoT), is predicted as future possibility that a huge amount of physical objects will become online. From a security point of view, the more devices are connected to communication networks, the more powerful cyber-attacks can be occurring. The main goal of this research is to design, develop and implement new attack detection model and enhance approaches for IoT.

The level of cyber-attacks increasing in volume and sophistication, the need for improved counter measures is growing. The impacts of a successful attack on a critical communications would result in a paralysing collision on the economy and the general population as a whole.

Though several approaches to detect intrusion have been already proposed, the area of clustering and categorization of packet signatures has potential scope for research. Whenever features of incoming network packet match
one of the signatures of intrusion, the system alerts the administrator about
the possible threat with details of source of malicious activity and the
classification is found to be more than 90% accurate.

Smart objects connected to the Internet, constituting the so called Internet of
Things (IoT), are revolutionizing human beings’ interaction with the world.
As technology reaches everywhere, anyone can misuse it, and it is always
essential to secure it.

Network Intrusion Detection Systems (NIDS) which should perform time-
consuming evaluation of every packet received from network have faced
throughput challenge as a result of the increase in the speed of network
communications and the high volume of Internet threats. In an NIDS, the
most important and time-consuming processes are pattern matching and
deep inspection of the header and the body of packets. Several analyses
show that this process can take up to 75% of the time of processing packets.

The rapid growth of computers transformed the way in which information
and data was stored. With this new paradigm of data access, comes the
threat of this information being exposed to unauthorized and unintended
users. Many systems have been developed which scrutinize the data for a
devention from the normal behavior of a user or system, or search for a
known signature within the data. These systems are termed as Intrusion
Detection Systems (IDS). Intrusion Detection is the process of monitoring
and identifying attempted unauthorized systems access or manipulation.
Successful High Performance Computing (HPC) requires a combination of
technical innovation as well as political and operational experience to
balance out the many (sometimes contradictory) pressures encountered in
this field. This is particularly true with respect to operational field.
Cloud computing is an enticing field nowadays due to its cost effective nature, easy accessibility, the pay per use service and shared resources. These shared resources, easy accessibility and shared storage of resources are responsible for putting the confidential information under a great deal of risk. Although the cloud is becoming gigantic day by day but its efficiency is being hampered considerably due to the threats in the cloud computing environment. The threats in the cloud computing environment not only account to external attacks which are launched with the intention of hampering work flow of the cloud provider but the internal attacks also which are being launched so that the efficiency and the reliability of the cloud is at stake. The firewalls monitor traffic between networks such that all the traffic must flow through it, but they are certainly not sufficient to shield the dynamic cloud computing environment from all attacks. They may be able to subvert external attacks to a certain extent but internal attacks do not even pass through the firewalls, therefore rendering them useless.

Moreover, attackers exploit vulnerabilities in the virtual machines (VM) in order to set up large scale attacks like Distributed Denial of Service (DDOS). They compromise these VM’s into zombies and the detection of these VM’s is very difficult because cloud users install all types of applications onto their VM’s some of which may be malicious.

In earlier period, we have seen that the rising speed of the network attacks compromising computer system functionality and lowering network performance. The security of these systems has attracted a lot of research in the field of intrusion detection and response system to reduce the effect of these attacks. Reaction is a main part of intrusion detection system. Intrusion detection system without a appropriate reaction is not measured good even they discover threat and produce alarms. Best possible reaction is based on the selection of proper reaction option.
The unyielding trend of increasing cyber threats has made cyber security paramount in protecting personal and private intellectual property. In order to provide the most highly secured network environment, network traffic monitoring and threat detection systems must handle real-time data from varied and branching places in enterprise networks. Though numerous investigations have yielded real-time threat detection systems, the issues to be addressed, the issue of handling the large volumes of network traffic data of enterprise systems, while simultaneously providing real-time monitoring and detection remain unsolved.

4.2 ADVANTAGES OF INTRUSION DETECTION SYSTEM

IDS are becoming the logical next step for many organizations after deploying firewall technology at the network perimeter. IDS can offer protection from external users and internal attackers.

4.2.1 Continuous Network Monitoring

Intrusion detection systems continuously monitor a given computer network for offensive or abnormal activity. The advantage of IDS service is the "24 hours monitoring" feature. The IDS safeguard the system even though the user is sleeping or otherwise away from any computer connected to the network. The user information, access to the network, and firewall measures and all other actively will be monitored by the intrusion detection systems.

4.2.2 Flexibility of the System

The Intrusion detection systems are especially able to accommodate exact client needs. This allows users to give custom-build network security to monitor each and every activity; from overt attacks to the network to
examining suspicious or specific patterns of activity which may be a masquerade attempt to penetrate system security from outside the network, or perhaps the work of someone inside the security network. The system is able, through customization, to monitor both the outside threats to a given network, and patterns of behavior which may be threats operating within the system. The network or computer is constantly monitored for any invasion or attack.

The main advantages of the Intrusion Detection Systems are

- The system can be modified and changed according to needs of specific client and can help outside as well as inner threats to the system and network.
- It effectively prevents any damage to the network.
- It provides user friendly interface which allows easy security management systems.
- Any alterations to files and directories on the system can be easily detected and reported.

The only disadvantage of Intrusion Detection System is they cannot detect the source of the attack in any case of attack; they just lock the whole network.

4.3 EXISTING METHODOLOGY

The Internet of Things (IoT) is an ever-growing network of smart objects. It refers to the physical objects are able to exchanging information with, other physical objects are able to exchanging information with other physical
objects. It begins various services in humans’s routine life depends on its available and reliable activities. The IoT requires strong security solutions where the communication is secured with confidentiality, integrity and authentication services; the network is protected against intrusions and disruptions. Generally, the data inside a sensor node is stored in an encrypted form. Therefore, the challenge of implementing secure communication in the IoT network must be more important. The IoT network is secured with encryption and authentication, but it cannot be protected against cyber attacks. Along with the development of Internet of Things (IoT), there are a lot of increasingly serious security problems. The traditional intrusion detection method cannot adapt to the requirement of IOT. The existing research for efficient IDS tool for IoT is at its infancy stage. Hence, an effective Intrusion Detection System is needed to secure IoT devices against cyber attacks.

The Security Problems of Internet of Things Internet of things (IOT) should use wireless transmission on many occasions, if it is not proper protection mechanism; the IoT network signal exposure in public places will easily be stolen, and easily be disturbed or hacked. This will directly affect the safety of the system of IOT. Perception nodes of IOT must be deployed in unattended scene. They cannot have complex security protection. So it is difficult to use the traditional computer network security algorithms and protocols the IoT. According to different functions, network architecture of IOT it is divided into three levels.

Underlying layer is used to information collected—perception level. The middle layer is the network layer used to data transmission. The top level is the application / middleware layer.
The information transmission in IOT generally is between the perception layer and network layer. In this situation it is easily to intrude and the intruders can fetch the information easily.. So we proposed ANSVN intrusion detection system to detect the data sent from the perception layer. So we can find timely detection of abnormal access. Requirements of intrusion detection system in IOT:

✓ The first is to reduce the computational.
✓ The second is to run faster, and Smaller Used memory.
✓ The third is to have a variety of training data, and requirements of Data integrity low.

Other considerations that will affect the IoT IDS deployments include encryption, IPv6, scalability and management, and deployment complexity. Deploying intrusion detection systems to identify attacks at layer three and above will have challenges. Intrusion detection relies on the ability to inspect packet payloads to search for content, and as more applications leverage encryption to maintain security and privacy, this will cause blindness in monitoring. To deal with encryption, there needs to be some type of key offload mechanism, where packets are decrypted and inspected. This can be costly and complex, and is a contentious issue. To better illustrate the detection capability, we can look at attacks against IoT environments and how intrusion detection can be used to identify attacks both in traditional IP networks, and in LoWPANs. Intrusion detection in IP based networks are fairly mature with standard detection mechanisms, however detection in wireless environments are less mature, and require a bit of tailoring for each scenario.
4.4 PROPOSED METHODOLOGY

Through the literature survey it is proposed that, an Artificial Neural Support Vector Network (ANSVN) can be used to identify threats with multi-level scanning. The IP based ANSVN algorithm is trained using internet packet traces, and then it may be deployed in the networks to identify network threats and intrusions of IoT. This algorithm is fully based on neural fuzzy artificial intelligence with support vector machine working methodology, so it can identify the position information of a node and its neighbour nodes to identify predefined wormhole attacks in the IoT. In this research, a proposal has been laid down for establishing and analyzing an artificial immune neural network for securing the IoT network architecture. The method used in decision-making converted to intelligent strategy based on knowledge support and is directed by the goal of problem solving. In the IoT, group of wireless devices, enveloping system and sensor based network are linked with new network service condition that inspire to analyze issues of several internet related problems and issues.

Figure: 4.1 IoT Intrusion Detection Architecture
In today’s competitive world, IoT security is at enormous demand due to tremendous amount of network attacks. These types of threats are considerably affecting the architectures of the network by gaining unauthorized access to the IoT networks. The Information Security is therefore necessitates the decrease of such attacks. In this paper, a proposal has been laid down for establishing and analyzing an artificial immune neural network for securing the IoT network architecture. The method used in decision-making converted to intelligent strategy based on knowledge support and is directed by the goal of problem solving. In the networks of computers, Internet of things (IoT) is a rising concept in which stylish and data -constrained devices can connect to Internet by using a large range of technologies. Because of the insecure environment of Internet and also wireless sensor networks (WSNs), which are the main gears of IoT, employing security mechanisms in IoT seems essential.

Figure: 4.2 ANSVN Block Diagram
Knowledge based database of our proposed model which learns vector representations form entries in a knowledge base in order to predict new IP base technology. By combining knowledge base with word representations, the relationships can be predicted with higher accuracy even the entities that are not available in the original knowledge base.

The goal of database configuration is to learn models for knowledge based reasoning ability to realize the fact of the existing relations that some facts hold purely due to other existing relations. Another way to describe the goal is link prediction in an existing network of relationships between entity nodes in sensor decision making mechanism.

4.5 FEATURES OF THE METHODOLOGY

The Neural Network and Support Vector Networks of computer systems that jointly deploy complex mapping functions. Through this Support Vector Procedure, the neural network is presented with labeled training set which learns a mapping from inputs x to outputs y. The Neural networks are a network of networks of computer systems that jointly deploy complex mapping functions. It is presented this neural network based approach for intrusion detection on IoT network to identify DDoS/DOS attacks.

Knowledge based database of our model which learns vector representations for entries in a knowledge base in order to predict new technology. A database is a large repository of facts, designed in such a way that processing the facts into information is easy. The system also acts as per the database configuration to learn models, for common sense reasoning, the ability to realize that some facts hold purely due to other existing relations. Another way to describe the goal is link prediction in an existing network of relationships between entity nodes in sensor decision making mechanism. This system presents a threat analysis of the IoT and uses Artificial Neural
network to face the threats on IoT. This system also focuses on the classification of normal and threat patterns on an IoT Network. The ANN procedure is validated against a simulated IoT network. The experimental results demonstrate high accuracy and can successfully detect various DDoS/DoS attacks.

4.6 METHODOLOGY DESIGN AND DEVELOPMENT

The operation of the intrusion detection system is fairly comparable as that of the other program used to stop the computer scheme from unsafe threats like malware, spyware, spam etc. The works of the intrusion detection system starts from the Wormhole attack footage to find the threat in some incident. When the scheme have the difficulty to monitor, then it sends to the management section of the intrusion detection scheme which makes more than a few preventive events to defend the system and keep the scheme in the safe hands. Intrusion detection system can work in the exact manner by monitor some significant safety things from the threats. These important things are as follows.

![Proposed Flow Chart](image)

**Figure: 4.3** Proposed Flow Chart
ANSVN Algorithm Initial process is as follows.

1: for all neighbors do
2: for all failure types do
3: if round-failure value > cumulative value then
4: signal attack indication
5: else
6: update cumulative value by combining t with round-failure value
7: end if
8: end for
9: end for

4.6.1 Proposed Methodology Flow Diagram

![ANSVN Flow Diagram](image)

**Figure:4.4** ANSVN Flow Diagrams

The proposed algorithm was divided into the following phases:

Phase 1 – Data acquisition: in this phase, messages are collected in a promiscuous mode and the important information is filtered before being stored, for subsequent analysis.
Phase 2 – Rule application: this is the processing phase, when the rules are applied to the stored data. If the message analysis fails the tests being applied, a failure is raised.

Phase 3 – Intrusion detection: this is the analysis phase when the number of raised failures is compared to the expected amount of occasional failures in the network. If the former is higher than the latter, a intrusion detection is raised.

4.7 Experimentation and Results:

The proposed algorithm is used with data neural technique of categorization with linear classifier. Detecting the unknown (wormhole attacks) means here it is comparing the signature of an attack with other type of signature. The data undergo two phases i.e. training and testing phase. In training phase, it has the number of entries to read.

In training phase, input entry number to be given to train datasets. The table records of both testing and training entries of data set and time required for manipulating the dataset.

Neural Networks with three dissimilar training functions by unreliable figure of nodes in next hidden layer to node is taken for calculation, this standard of SVN is taken as the mixture of all attack and normal family member recognized properly by the classifier. The ANSVN achieve through IDS neural network using preparation purpose “train” is higher as contrast to other two neural network by unreliable nodes in second hidden layer. The overall alliance percentage is reduced for all networks as compared. The results obtained in the proposed system are given in the following Figure and table.
Table 4.1 IoT Intrusion identification based on IP

<table>
<thead>
<tr>
<th>S.No</th>
<th>Time</th>
<th>Destination</th>
<th>Bytes</th>
<th>Source</th>
<th>Allowed/ Not Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.514756</td>
<td>192.168.1.5</td>
<td>195</td>
<td>192.168.1.0</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>2</td>
<td>5.732525</td>
<td>192.168.1.5</td>
<td>195</td>
<td>192.168.1.1</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>3</td>
<td>6.425259</td>
<td>192.168.1.5</td>
<td>195</td>
<td>192.168.1.4</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>4</td>
<td>7.931522</td>
<td>192.168.1.5</td>
<td>195</td>
<td>192.168.1.2 ec:01:ee:d1:5e:oa</td>
<td>Allowed IoT device</td>
</tr>
<tr>
<td>5</td>
<td>8.312821</td>
<td>192.168.1.5</td>
<td>195</td>
<td>192.168.1.3</td>
<td>Not Allowed</td>
</tr>
</tbody>
</table>

Figure 4.5: Number of Legitimate Nodes and Malicious Nodes
4.8 Conclusion

A move toward for a neural network based intrusion detection system to classify the usual and attack pattern and the type of the assault is proposed. When the neural network parameter was strong-minded by training, categorization of a single record was done in an insignificant time. The proposed system present an implementation of IDS in threat detection over network security and monitor the threat packet signature like wormhole attack in different scenario by use of ANSVN (Artificial Neural Support Vector Network) approach of intrusion detection system based on neural network. The screenshots for packet capture, ANSVN tool, throughput, end to end delay, energy efficiency, time taken to detect malicious nodes are explained elaborately in the appendix I. Hence ANSVN algorithm is designed and experimented using IoT network with limitations. The experimentation result provides good solution to protect IoT networks.