CHAPTER 6

6. CONCLUSIONS AND FUTURE WORK

In this thesis, it is addressed that the issues of intrusions in WSN, IoT and Big Data. Many algorithms have been proposed earlier, but the proposed algorithms for WSN, IoT and Big Data has given efficient detection mechanism. So here the discussions of conclusions arrived from the results of the previous sections and suggested future research directions.

6.1 INTRODUCTION

In order to overcome various types of attacks on the computer systems in the WSN, IoT networks and Big Data an effective Intrusion Detection Algorithms for WSN, IoT Network and Big Data Systems are developed and experimentally tested. The extract of the findings is presented in this section.

In current internet network scenario wireless network which uses license free Wi-Fi band along with WSN, IoT network enhances the connectivity of the enterprise user and adds various threats. To combat with such network threats, the design of a Intrusion Detection System and Packet Analyzer Tool becomes a challenging task. There are many open topics in security for IoT networks, for instance, encryption algorithms, authentication, intrusion detection, intrusion prevention, visualization, location and so on. The aim of the research work is to appraise the current situation relating to the problems in Intrusion in WSN, IoT network, and Big Data and also the entire research work reported in this thesis is based on the experimental set up results to provide WSN, IoT network and Big Data Systems security.

Unofficial network devices linking to the network through AP can engage in information or data theft, rerouting, data or information corruption,
impersonation, DoS, virus insertion, and many other types of attacks on the
computer systems in the network. Thus, it is a real requirement to have
Intrusion Detection system whether the network is belongs to WSN, IoT or
Big Data. The network security is divided into various implications, such as
IDS for WSN, IoT Network, Big Data Systems. This necessitates the
development of a new Intrusion Detection System by taking into account the
above mentioned factors to ensure WSN, IoT and Big Data security.

6.2 CONTRIBUTION OF THE THESIS

In order to overcome various types of attacks on the computer systems in the
WSN, IoT networks and Big Data, Intrusion Detection Algorithms for WSN,
IoT Network and Big Data Systems are developed and experimentally
tested. The excerpt of the findings is presented in this section.

6.2.1 Development of ASVM Algorithms for WSN

A wireless sensor network may consist of thousands of sensor nodes. Each
sensor node has a sensing capacity as well as limited energy supply,
compute power, memory and communication ability. Besides military
applications, wireless sensor networks may be used to monitor
microclimates and wildlife habitats the structural integrity of bridges and
buildings, building security, location of valuable assets (via sensors placed
on these valuable assets), traffic, and so on. However, realizing the full
potential of wireless sensor networks poses countless challenges ranging
from hardware and architectural issues, to programming languages and
operating systems for sensor networks. For the security reasons of WSN
development of new algorithms is essential.
So it is proposed a new Advance support vector machine algorithm (ASVM) to eliminate the existing drawbacks such as active and passive attacks because of its open medium, fast changing topology, lack of centralized monitoring system etc. and also they can only detect the intrusions only as per limited assumptions. The main focus of this research is to detect internal attacks; there is no proper implementation for internal attack, so the existing technology is not fair. Intrusion detection system (IDS) is used to monitor the malicious traffic in a particular node or network. But there is much challenge to implement the IDS in sensor Networks. Through the ASVM algorithm it is possible to find abnormal packets based on its false misbehavior data report and detect abnormal IP packets and give alarm.

Due to the ASVM classification of sensors the overall system runs faster for example it acts like Queue to reach destination faster. Sensor events which perform data collecting agent from sensors nodes in FIFO concept to receive the data. The external attack which arrives suddenly without any intimation which collapse the overall network topology so to avoid this situation it is recommended to ensure the ASVM algorithm which plays a role like to stop the attack and alert the overall system.

The “Advance Support Vector Machine” (ASVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this proposed algorithm, it differentiates the normal and abnormal IP based data flow in network topology. Then, the ASVM Algorithm performs classification by finding the attack plane. The Classifier acts like trigger mechanism to alert the system from the intrusion.
6.2.1.1 Experimental Analysis and Results of ASVM Algorithm on WSN

ASVM defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. When Abnormal IP enters in the IDS the IDS will filter the abnormal packets. When the number of malicious nodes increased, packet delivery system gradually slowed down. The tests are conducted based on the IP to distinguish the normal and abnormal IP’s.

Security is the most important anxiety for WSN researchers and designer because of its serious applications in different environments. In this research we discuss the security issues, a variety of security attacks and their counter measures. So we analyzed the review of recent work on dissimilar approaches of IP based IDS for WSN. It has been experimented that these intrusion detection systems are not sufficient for defensive WSN from intruders professionally. It is found that various IDS approaches to detect those internal malicious attacks. Those approaches have some limitations for the detection of attacks. There is no proper solution to detect internal attacks of WSN network. It is expected that the proposed solution will greatly help to detect internal malicious attacks in real time.

The tests are conducted based on the IP using our ASVM algorithm to distinguish the normal and abnormal IP’s. The test results show that the proposed method provides a good solution to protect WSN.

6.2.1.2 CONCLUSION

The experimentation conducted on this WSN gives the following conclusion:
Intrusion happens when there is change in the hash value generated in the source connected system and it will infect all the system connected in the WSN or IoT Network, and automatically decreases the overall performance of the all the connected system. The abnormal packets were generated and sent to experimental setup system. ASVM defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. When Abnormal IP enters in the IDS the IDS will filter the abnormal packets. The experimentation screenshots presented in the appendix –I and the test results show that the proposed method provides good solution to protect WSN. Thus, our paper “A novel scheme to Identify Intrusions by using ASVM Algorithm in WSN” has been published in the International Journal of Technology in Computer Science & Engineering and the Intrusion Detection System for WSN has detected abnormal packets when experimented and its versatility in WSN is validated.

6.2.2 Development of ANSVN Algorithms for IoT

There are many predications on IoT that there will be at least 10 billions of IoT devices connected by 2020. But each and every IoT devices connected increases the risk of privacy and security threats. These threats range from hackers stealing our information and even threatening our lives. But the usage of IoT will not be stopped. The basic security weakness of Internet of Things is that it increased the number of devices. Internet of Things (IoT) make over network communication to Machine-to-Machine (M2M) basis and offers open access and new services to general public and companies. It expands the border of Internet and will be developed as one part of the future 5G , 6G networks. However, as the resources of IoT’s front devices are constrained, many security mechanisms are hard to be implemented to protect the IoT networks. Intrusion detection system (IDS) is an efficient technique that can be used to detect the attackers when coding and decoding
is broken, and it can be used to enforce the security of IoT networks. In this research, we analyzed the intrusion detection requirements of IoT networks and then we proposed an Artificial Neural Support Vector Network (ANSVN) to identify these threats by multi-level scanning. The 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 working methodology, so it can identify the position information of node and its neighbour node to identify predefined wormhole attacks in the IoT and also identify malicious nodes of IoT.

6.2.2.1 Experimental Analysis and Results of ANSVN Algorithm on IoT

Internet of Thing’s 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 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. 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 senior decision making mechanism.

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. 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.
The proposed algorithm is used with data neural technique of categorization with linear classifier. Detecting the unknown (wormhole attacks) means here we are 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 enter the number of entries to read. In training phase, input entry number to be given to train data sets. The table record 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.

6.2.2.2 CONCLUSION

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. Artificial intelligence is widely used in decision making system and classification purposes. The neural network generates results that are more accurate. The abnormal packets were generated and sent to experimental setup system. When Abnormal IP enters in the IDS the IDS will filter the abnormal packets. Here we presented ANSVN algorithm implemented and experimentation screenshots are presented in appendix- I. The test results show that this proposed method provides good solution to protect IoT devices. Thus, the paper “Development of Intrusion Detection
System for Threat Identification of Internet of Things using ANSVN” has been published in the International Journal of Technology in Computer Science & Engineering and the Intrusion Detection System for IoT has detected abnormal packets when experimented and its versatility in IoT is validated.

### 6.2.3 Development of AHSVN Algorithms for Big Data

Drastic growth in data size, data complexity, and data rates, triggered by coming out of high-throughput technologies such as remote sensing, crowdsourcing, social networks, or computational advertising, in recent years has led to an increasing availability of data sets of extraordinary scales, with billions of high-dimensional data examples stored on hundreds of terabytes of memory. In order to make use of this large-scale data and extract useful knowledge, researchers in machine learning and data mining communities are faced with numerous challenges, since the data mining and machine learning tools designed for standard desktop computers are not capable of addressing these problems due to memory and time constraints. As a result, there exists an evident need for development of novel, scalable algorithms for big data. And also Network hacking crime is going on increasing since the available security technologies are not performed well in big data environment. Due to the increasing cyber attacks, constructing Hybrid intrusion detection system is necessary for preventing from attacks. But the multiple IDS approach to co-exist in a single system is a major challenging task. To overcome this issue, it is proposed an Adaptive Hybrid Support Vector Network Algorithm (AHSVN). This mechanism used in the Intrusion Detection scheme helps to identify the attack at the early stage and give alarms and also the node will generate alerts to other nodes if there is a possibility of attack.
6.2.3.1 Experimental Analysis and Results of AHSVN Algorithm on Big Data

The cyber attacks go on increasing due to the existing IDS technologies which are not capable of detecting the intrusions. The proposed work will enrich the efficiency of the IDS as compare with the earlier IDS systems. The main work of this research paper is maintaining security across the external fraud detection data from homogeneous sources and co-relating the heterogeneous data from different sources using hybrid strategy over Big Data. The proposed system specifies a set of IP base rules AHSVN in Hadoop concept one can attempt to get good results by improving the efficiency and reducing the complexity present in the model of external unknown attacks. The main purpose of IDS is to identify suspicious or malicious activity, note activity that deviates from normal behavior, catalogue and classify the activity, and if possible, respond to the activity.

Signature based approach block finds out the intrusion activity in existing packet with the help of attack rules and if found then applies appropriate rules otherwise it drops the packet. It takes different time to respond different packets that depends upon the power of machine and number of rules defining the system. The AHSVN block has detection engine that might generate an alert or used to do log activities. Depending upon the nature of data all log files are kept by default in a folder and by using command line options the location can be changed.

The output modules save output generated by the logging and alerting system of AHSVN. The administrator will get the alert from the IDS by database searching and query building by AHSVN Algorithm. Searches can be performed between network specific parameters such as the attackers
internet protocol address, and other parameters such as time or date of an event, by AHSVN triggered rules.

Advance Pattern analysis includes categorization which enclose support vector network algorithm. Support Vector Network is clustering algorithm which is used for discovery of network attacks. Support Vector Network is second-hand for intrusion detection system to notice which IP has viruses and then clean that IP packet.

The IP based Hybrid support vector network is a new learning machine algorithm. In Hybrid Support Vector Network algorithm, data set is divided into preparation part and testing part. The existing methodology has high error rate. So the AHSVN classify the attacks using support vector network learning algorithm. The major reasons for using AHSVN in IDS are speed. AHSVN can learn a larger set of patterns and can scale better than any existing methods. Feature selection or attribute reduction can help to reduce the SVM classification time and saving memory space effectively and efficiently.

6.2.3.2 CONCLUSION

To protect from various threats in Big Data analysis system, data sets have been analyzed with our new technique, IP based Adaptive Hybrid Support Vector Network algorithm to prevent external unknown attacks. The proposed approach mainly focuses on unknown external fraud detection in big data, using Adaptive Hybrid Support Vector Network algorithm (AHSVN). The experimentation screenshots are presented in the appendix-I shows that using the proposed method improves the performance of the system. When Abnormal IP enters in to the IDS the IDS will filter the abnormal packets and give alerts. Thus, our paper “Development of Hybrid
Intrusion Detection System on Big Data for Detecting Unknown attacks by using AHSVN” has been published in the International Journal of Technology in Computer Science & Engineering and the Intrusion Detection System for IoT has detected abnormal packets when experimented and its versatility in IoT is validated.

6.3 FUTURE RESEARCH DIRECTIONS

Our future research directions is to build a real time Wireless Sensor Network, Internet of Things and Big Data (WITB) IDS and Protection tool to counter the new security threats posed by WSN, IoT, and Big Data network. The future research direction is to build a real time WITB protection tool captures the IP packet using an ASVM, ANSVN and AHSVN algorithms and can be named as ASANAH and links to a database. A front end is created to visualize the incoming packets in an enterprise network comprising of wired and wireless connected computers. The future enhancement tool is proposed dynamically and intimates the intruders details along with packet flow details. The ASVM Algorithm can find normal and abnormal IP packets and based on the finding, the IDS tool will take appropriate action against the alert. The Future real time work of ANSVN Algorithm can find normal, abnormal partially affected and fully affected IP packets. The Future real time work of AHSVN Algorithm can find mixed threats such as normal, abnormal, partially affected, fully affected, internal attack, external attack, repeated attack and virus attack. The Future work can be incorporated with an IP Trace back tool to trace the route of the intruder in real-time.
Thus, this research work concludes with the contributions of experimental study and their related results on Advance Support Vector Machine Algorithm (ASVM), Artificial Neural Support Vector Network (ANSVN), Adaptive Hybrid Support Vector Network Algorithm (AHSVN) and all these results have been published.