# DEVELOPMENT OF INTRUSION DETECTION SYSTEM FOR THREAT IDENTIFICATION OF INTERNET OF THINGS using ANSVN

S. Ramesh [1]
Research Scholar
Manonmaniam Sundaranar University,Tirunelveli, T.N, India
ramesh20062000@gmail.com

Dr. H. Abdul Rauf [2]
Dean & Professor, Department of CS & Technology
Sri Sastha Institute of Engineering and Technology, Chennai, T.N, India
harauf@yahoo.com

Dr. S.P. Victor [3]
Dean of Science & Associate Professor of Computer Science
St. Xavier's College, Palayamkottai, T.N, India
drspvictor@gmail.com

**Abstract:** The Internet of Things (IoT) is an ever-growing network of smart objects. It refers to the physical objects which are capable of exchanging data with other physical objects. The IoT introduces various services, currently most of the day to day life depends on its available and reliable activities. Each and every single device and sensor in the IoT signifies a possible risk. The major challenges in IoT are Vulnerability, Trust and Data integrity, Data collection, Protection and Privacy. Therefore, the challenge of implementing threat identification in the IoT network is essential. The IoT network is secured with encryption and authentication, but it cannot be protected against cyber-attacks. Therefore, the Intrusion Detection System (IDS) for threat identification is needed to secure communication of IoT networks. To overcome these challenges we propose 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 by using Received Signal Strength Indicator (RSSI). We have tested the feasibility of the ANSVN algorithm using Network Simulators (NS2 & NS3). The test result shows that this approach act against sophisticated attack by improving accuracy, precision rate and reduce the false positive rate and keep guard data integrity, confidentiality and availability of IoT.
**Keywords:** ANSVN, IoT, RSSI

## 1. Introduction

The level of cyber-attacks increasing in volume and sophistication, the need for improved counter measures is growing. The repercussions of a successful attack on a critical infrastructure would result in a paralysing impact on the economy and the general population as a whole.[1]

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.[2]

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.[3]

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.[4]

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 deviation from the normal behaviour 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.[5]

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.[6]

In past decades, we have seen that the increasing speed of the network attacks compromising computer system functionality and degrading 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. Response is a major part of intrusion detection system. Intrusion detection system without a timely response is not considered good even they detect threat and generate alarms. Optimum response is based on the selection of proper response option.[7]

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.[8]

## 2. Literature Survey

In 2012, **William Hurst, Madjid Merabti** et al. concluded that the seriousness of critical infrastructure protection is clearly a key issue. Their vulnerability to the growing cyber threat enforces this further. Defence in

depth is a prominent factor which must be taken into account when developing security and also proposed to provide functional support and enhance security. Through the development of a model of expected acceptable behaviour, by combining the network activity with the operational running of the infrastructure, threats can be identified.

In 2013, **Prabhakaran Kasinathan, Claudio Pastrone** et al. proposed the DoS detection architecture, built on top of the ebbits network framework was proved capable of detecting DoS attacks. It is more applicable to real world scenarios. Integrating information from the network manager components will increase the accuracy of attack detection. Nevertheless, in future more complicated attacks can be detected by using our DoS detection architecture. Since, our IDS runs on a host computer, it overcomes the resource constraint problems and provides more power to detect complicated attacks. It showed promising results and unearthed new ways to detect more complicated attacks related to 6LoWPAN, which could have not been possible earlier.

In 2013, **Ambarish Jadhav, Avinash Jadhav** et al. proposed network intrusion detection framework provides ability of clustering signatures to prepare a more solid protection against potential network attacks. The framework also proposed a new data pre-processing approach in which extracted about 25 different features from packets received and categorized them according to the severity of potential threat using the concept of fuzziness. An interesting avenue for future work is predicting what kind of network patterns lead to vulnerabilities in the system by periodically analyzing the data collected in network information tables. This will also help incrementally build the signature database.

In 2013**, Payam Mahdinia, Mehidi Berenjkoob** et al. proposed a novel method which aims to port a rule signature-based search engine as the most time-consuming part of IDS to GPU in order to solve the problem of losing traffic in high-performance IDS systems. In this method, instead of the commonly used Aho-Corasick algorithm, PFAC string matching algorithm has been used and considering the need for complete evaluation of rules. This method provides a means to perform payload matching and non payload matching of packets in a parallel platform on GPU, which can speed up the signature-based detection engine of Snort 3.6.

In 2014, **Brojo Kishore Mishra, Minakshi Sahu** et al. concluded the intrusion detection and intrusion prevention arenas are extremely dynamic, with new findings, functions, and models being created all the time. A considerable amount of research on data visualization methods for intrusion detection data is also currently being conducted. At some point, the major breakthroughs from this research will be incorporated into IDSs of the future, resulting in output that will be much more useful in terms of identifying threat magnitudes, patterns of elements within incidents, and so forth. It also showed how intrusion detection can benefit from high performance computing techniques.

In 2014, **Rutba Maqsood, Naila Shahabuddin** et al. proposed an intrusion detection system which detects the intrusions launched on the VM's which act an avenue for deploying large scale attacks, therefore, minimising the loss. The proposed IDS is a network IDS and provides security from the IaaS based attacks. Data security is one of the major challenges of cloud computing environments, thus, for enhancing data security AES algorithm is used. Moreover, additional backup and recovery options are provided for minimal data loss. The cloud computing environment is so diverse and so enormous, that no security mechanism will ever be sufficient. There will always be new attacks and new vulnerabilities will arise with the growth of the cloud. The IDS given in the paper is network IDS which detects attacks on the VM. This IDS provides security from the Internet as a Service (IaaS) based attacks.

In 2015, **Shahid Anwar, Jasni Muhamad Zain** et al. proposed optimum response option based on the attacks' statistics during the response selection process. In addition, the selection of optimum response option will improve the overall performance of IDS.

In 2015, **VenkataRamesh Bontupalli Tarek M.Taha** et al. concluded that Intrusion detection is the most popular research topic in network security and various machine learning techniques and its methods have been explored to detect intrusion. The successful growth of intrusion detection with the help of artificial intelligence techniques brought a great literature to the IDS methodology. A study of stock of its research methods help us to

estimate the loop holes in the current trend and helps to mitigate them. It also helps to propose more methods and solution for developed intrusion detection and target the open problem existing in the field. The self-learning approaches like Artificial Neural networks (ANN), Support Vector Machines (SVM), K-Nearest Neighbour (KNN) combining multi criteria decision trees like C.45, and OneR may bring much benefit for intrusion detection. However, Memristive based IDS proved to be very effective in terms of detection accuracy, high throughput and extreme low power.

In 2015**, Fang-Yie Leu,Kun-Lin Tsai** et a.l proposed an approach that employs data mining and forensic techniques to identify the representative SC-patterns for a user. The time that a habitual SC pattern appears in the user's log file is counted, the most commonly used SC-patterns are filtered out and then a user's profile is established. By identifying a user's SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers. The experimental results demonstrate that the average detection accuracy is higher than 94% when the decisive rate threshold is 0.9, indicating that the IIDPS can assist system administrators to point out an insider or an attacker in a closed environment.

In 2016, **Zhijiang Chen,Hanlin Zhang** et al. proposed a streaming-based network monitoring and threat detection system to manage significant network traffic data streams and also introduced a cloud computing model utilizing Flume, Sharp, and Hadoop to efficiently analyze streaming network data. The implementation includes Streaming k-means and Fuzzy c-means algorithms for the purpose of clustering normal and abnormal data in order to extract malicious network traffic. Through our evaluations of threat detection and system performance, demonstrated the viability of the proposed system in real-time detection for enterprise networks.

## 3. Objective

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 working methodology, so it can identify the position information of a node and its neighbour nodes to identify predefined wormhole attacks in the IoT. It also identifies malicious nodes of IoT by using Received Signal Strength Indicator (RSSI).

In the IoT, group of wireless devices, enveloping system and sensor based network are linked with new network service condition that inspire to analyse issues of several internet related problems and issues.

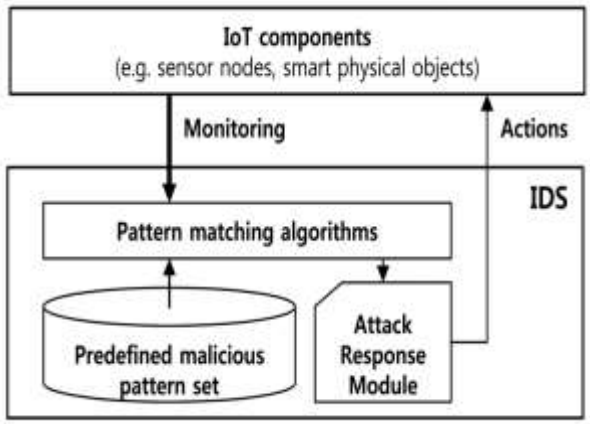


Fig: 6 IoT Intrusion Detection Architecture

## 4. Proposed Methodology Block Diagram

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.

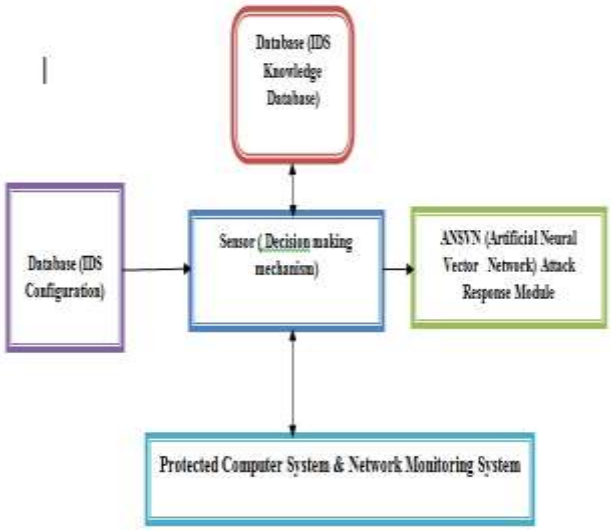


**Fig: 1** Block Diagram

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 senor decision making mechanism**.**

## 5. Design and Implementation

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.

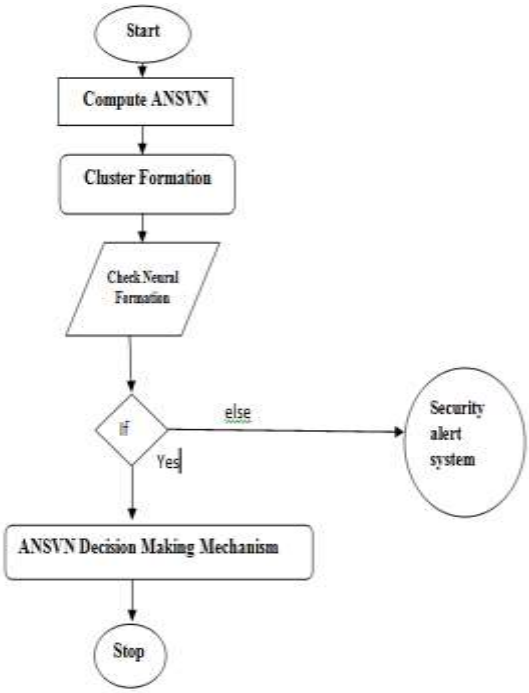


**Fig: 2** Proposed Flow Chart

**5.1 ANSVN Algorithm Initial process**

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**

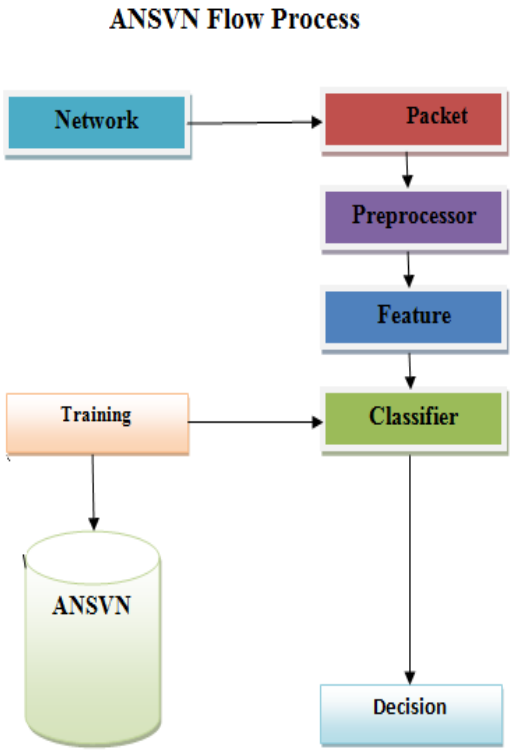


**Fig: 3** ANSVN Flow Diagrams

- Network is our ultimate protocol link layer to classify the process in step by step: Packet == node (i.e) frame to frame data send to application layer.
- Preprocessor the state transition analysis technique compares data against signatures
- Each packet is applied to a finite state machine following transitions until a final state is reached, hence detecting an attack.
- Feature and classifier play a important role in the IDS of the ANN are used to classify complex data flow. Maximum attacks is identified by Evaluating the complexity and it is done by setting the input nodes in a feed-back process and the event streams are propagated through the network to the output where it is classified as normal or compromised.

## 6. Experimental Results

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, we enter the number of entries to read.

In training phase, we enter number of entries to train data sets. We draw a table of both testing and training entries of data set and time required for manipulating the dataset. Below table shows the entries for testing and training datasets along with time required.

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 table and graph.

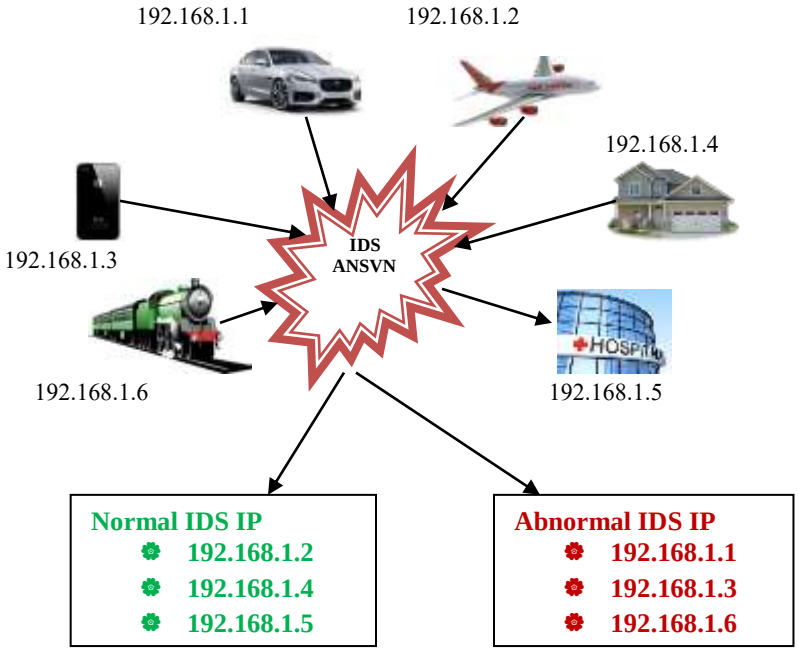


**Fig 5:** IoT Intrusion based on IP

| Time (ms) | Bytes | IP | Abnormal IP IDS | Normal IP IDS |
|---|---|---|---|---|
| 12:30:110 | 74 | 192.168.1.1 | 192.168.1.1 | |
| 12:31:110 | 74 | 192.168.1.2 | | 192.168.1.2 |
| 12:32:110 | 74 | 192.168.1.3 | 192.168.1.3 | |
| 12:33:110 | 74 | 192.168.1.4 | | 192.168.1.4 |
| 12:34:110 | 75 | 192.168.1.5 | | 192.168.1.5 |
| 12:35:110 | 75 | 192.168.1.6 | 192.168.1.6 | |

**Table: 3** Intrusion Detection based on IP

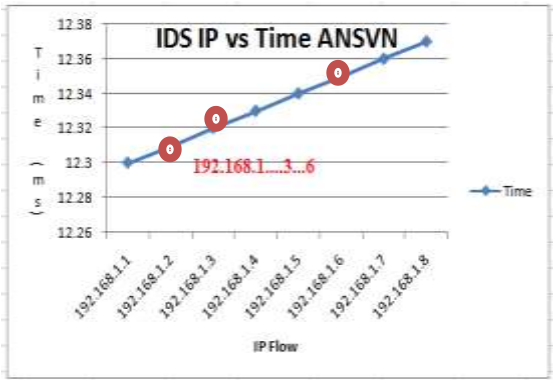


**Fig: 4** Graph Analysis Flow over IDS

## 7.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. Artificial neural network are enthused by the knowledge process that get put in biological systems Detection System along with features of an ideal intrusion detection system. We discussed the Support Vector Machine to deal with the classifier construction problem. Further there is need to design the system which will overcome the current challenges of IDS and also the system must provide a high performance in detecting the threats and security attacks.

## 8. Future work

The accuracy of the test reports can be improved in future by introducing new concepts and techniques in our system.In future a real time Intrusion Detection system for IoT to be experimented is proposed.

## 9.Reference

[1] William Hurst, Madjid Merabti, Paul Fergus “Operational Support for Critical Infrastructure Security” 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems Pages: 1473 - 1478, DOI: 10.1109/HPCC.2012.215

[2] Ambarish Jadhav, Avinash Jadhav, Pradeep Jadhav, and Prakash Kulkarni “A novel approach for the design of network intrusion detection system(NIDS)” PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System Pages: 22 - 27, DOI: 10.1109/SNS-PCS.2013.6553828

[3] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, and Mark Vinkovits “Denial-of-Service detection in 6LoWPAN based Internet of Things 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) Pages: 600 - 607, DOI: 10.1109/WiMOB.2013.6673419

[4] Payam Mahdinia, Mehdi Berenjkoob, and Hedayat Vatankhah "Attack signature matching using graphics processors in high-performance intrusion detection systems” 2013 21st Iranian Conference on Electrical Engineering (ICEE) Pages: 1 - 7, DOI: 10.1109/IranianCEE.2013.6599567

[5] Brojo Kishore Mishra, Minakshi Sahu, and Satya Naryan Das “Intrusion detection systems for High Performance Computing environment 2014 International Conference on High Performance Computing and Applications (ICHPCA) Pages: 1 - 6, DOI: 10.1109/ICHPCA.2014.7045369

[6] Rutba Maqsood, Naila Shahabuddin, and Divya Upadhyay "A Scheme for Detecting Intrusions and Minimising Data Loss in Virtual Networks" 2014 International Conference on Computational Intelligence and Communication Networks Pages: 738 - 743, DOI: 10.1109/CICN.2014.160
[7] Shahid Anwar, Jasni Muhamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Aws Naser Jabir, and Julius Beneoluchi Odili "Response option for attacks detected by intrusion detection system 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS) Pages: 195 - 200, DOI: 10.1109/ICSECS.2015.7333109
[8] Zhijiang Chen, Hanlin Zhang, William G. Hatcher, James Nguyen, and Wei Yu "A streaming-based network monitoring and threat detection system" 2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA) Pages: 31 - 37, DOI: 10.1109/SERA.2016.7516125
[9] VenkataRamesh Bontupalli, Tarek M. Taha "Comprehensive survey on intrusion detection on various hardware and software" 2015 National Aerospace and Electronics Conference (NAECON) Pages: 267 - 272, DOI: 10.1109/NAECON.2015.7443081
[10] VenkataRamesh Bontupalli, Tarek M. Taha "Comprehensive survey on intrusion detection on various hardware and software" 2015 National Aerospace and Electronics Conference (NAECON) Pages: 267 - 272, DOI: 10.1109/NAECON.2015.7443081
[11] Caiming Liu, Jin Yang, Run Chen, Yan Zhang, and Jinquan Zeng "Research on immunity-based intrusion detection technology for the Internet of Things" 2011 Seventh International Conference on Natural Computation Year: 2011, Volume: 1 Pages: 212 - 216, DOI: 10.1109/ICNC.2011.6022060
[12] Federica Paci, Carmen Fernandez-Gago, and Francisco Moyano "Detecting Insider Threats: A Trust-Aware Framework" 2013 International Conference on Availability, Reliability and Security Pages: 121 - 130, DOI: 10.1109/ARES.2013.22
[13] David Grochocki, Jun Ho Huh, Robin Berthier, Rakesh Bobba, William H. Sanders, Alvaro A. Cárdenas, and Jorjeta G. Jetcheva "AMI threats, intrusion detection requirements and deployment recommendations" 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm) Pages: 395 - 400, DOI: 10.1109/SmartGridComm.2012.6486016
[14] Peng He, George Karabatis "Using semantic networks to counter cyber threats" 2012 IEEE International Conference on Intelligence and Security Informatics Pages: 184 - 184, DOI: 10.1109/ISI.2012.6284294
[15] N. Wattanapongsakorn, E. Wonghirunsombat, C. Charnsripinyo, T. Assawaniwed, V. Hanchana, and S. Srakaew "A Network-Based Internet Worm Intrusion Detection and Prevention System" 2013 International Conference on IT Convergence and Security (ICITCS) Pages: 1 - 4, DOI: 10.1109/ICITCS.2013.6717779
[16] Sreenivas Sremath Tirumala, Hira Sathu, and Abdolhossein Sarrafzadeh "Free and open source intrusion detection systems: A study" 2015 International Conference on Machine Learning and Cybernetics (ICMLC), Volume: 1 Pages: 205 - 210, DOI: 10.1109/ICMLC.2015.7340923
[17] Sanjiban Sekhar Roy, P Venkata Krishna, and Sumanth Yenduri "Analyzing Intrusion Detection System: An ensemble based stacking approach" 2014 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) Pages: 000307 - 000309, DOI: 10.1109/ISSPIT.2014.7300605
[18] R. Ravinder Reddy, Y. Ramadevi, and K. V. N Sunitha "Effective discriminant function for intrusion detection using SVM" 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) Pages: 1148 - 1153, DOI: 10.1109/ICACCI.2016.7732199
[19] Weiming Tong, Lei Lu, Zhongwei Li, Jingbo Lin, and Xianji Jin "A Survey on Intrusion Detection System for Advanced Metering Infrastructure" 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC) Pages: 33 - 37, DOI: 10.1109/IMCCC.2016.193
[20] Divyatmika, Manasa Sreekesh "A two-tier network based intrusion detection system architecture using machine learning approach" 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) Pages: 42 - 47, DOI: 10.1109/ICEEOT.2016.7755404
[21] Daniel Kavan; Klára Škodová; Martin Klíma Network-based intrusion prevention system prototype with multi-detection: A position paper 2014 11th International Conference on Security and Cryptography (SECRYPT)
[22] Frantz Cadet; Daniel T. Fokum Coping with denial-of-service attacks on the IP telephony system SoutheastCon 2016 Pages: 1 - 7, DOI: 10.1109/SECON.2016.7506691

[23] Preeti Mishra; Emmanuel S. Pilli; Vijay Varadharajan; Udaya Tupakula Efficient approaches for intrusion detection in cloud environment 2016 International Conference on Computing, Communication and Automation (ICCCA) Pages: 1211 - 1216, DOI: 10.1109/CCAA.2016.7813926
[24] Automatic brain cognitive control detection method Bo Yu; Hai-feng Li; Lin Ma; Xun-da Wang International Conference on Software Intelligence Technologies and Applications & International Conference on Frontiers of Internet of Things 2014 Pages: 256 - 260, DOI: 10.1049/cp.2014.1571
[25] Xiaorui Wang; Qingxian Wang; Xiaolong Hu; Jianping Lu Security technology in virtualization system: State of the art andfuture direction IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012) Pages: 1 - 7, DOI: 10.1049/cp.2012.2392

[26] Systems for Detecting Advanced Persistent Threats: A Development Roadmap Using Intelligent Data Analysis Johannes de Vries; Hans Hoogstraaten; Jan van den Berg; Semir Daskapan 2012 International Conference on Cyber Security Pages: 54 - 61, DOI: 10.1109/CyberSecurity.2012.14
[27] Survey of learning methods in intrusion detection systems Abdulla Amin Aburomman; Mamun Bin Ibne Reaz 2016 International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES) Pages: 362 - 365, DOI: 10.1109/ICAEES.2016.7888070
[28] Nen-Fu Huang; Chuang Wang; I-Ju Liao; Che-Wei Lin; Chia-Nan Kao An OpenFlow-based collaborative intrusion prevention system for cloud networking 2015 IEEE International Conference on Communication Software and Networks (ICCSN) Pages: 85 - 92, DOI: 10.1109/ICCSN.2015.7296133
[29] Alaa Hussein Al-Hamami; Ghossoon M. Waleed Al-Saadoon Development of a network-based: Intrusion Prevention System using a Data Mining approach 2013 Science and Information Conference Pages: 641 - 644 Cited by: Papers (1) IEEE Conference Publications
[30] Elike Hodo; Xavier Bellekens; Andrew Hamilton; Pierre-Louis Dubouilh; Ephraim Iorkyase; Christos Tachtatzis; Robert Atkinson Threat analysis of IoT networks using artificial neural network intrusion detection system 2016 International Symposium on Networks, Computers and Communications (ISNCC) Pages: 1 - 6, DOI: 10.1109/ISNCC.2016.7746067