Intrusion Detection System : A survey

[1]Mrs. Asma A. Shaikh, [2] Dr. Devulapalli Sita

[1]Research Scholar, [2]Professor,

[1] Amity School of Engineering & Technology, Amity University Mumbai

[2]Amity School of Engineering & Technology, Amity University Mumbai

Abstract : Now days, information security is the major focus area of every organization because every organization moving towards Computer and Automation. Networks are open and distributed in nature that is more vulnerable to intruders. Along with these challenges, the number of attacks are also increasing exponentially due to the attack surface increasing through numerous interfaces offered for each service. . So to provide security there are different security approaches provided like firewalls, anti-virus etc. To provide security for network only firewall and antivirus is not sufficient so we need something which gives more security to the network so Intrusion Detection System is used.This literature review aims to provide researchers with a survey of existing dataset, Intrusion Detection Systems (IDS) and techniques capabilities and assets.

IndexTerms **– Intrusion Detection, Network Security**

I. INTRODUCTION

Intrusion Detection System (IDS) is most useful technique to identify harmful things which affect operations in the network. It is very crucial part of the network. Intrusion Detection System performed analysis of attacks[19].

Intrusion Detection System (IDS) is used to detect attacks on Network, Cloud, IOT devices. This research paper provides an overview of different intrusions in the network . Then, this analyze some existing intrusion detection systems (IDS) with respect to their type, detection technique, data source and attacks they can detect.

Depending on the type of analysis carried out , intrusion detection systems are classified as either signature-based or anomaly-based[1]. Signature-based schemes(also denoted as misuse-based) defined patterns, or signatures, within the analyzed data. To find attacks in the signature based IDS , a signature database of known attacks is prepared. Anomaly-based detectors is kind of IDS system where it matches predefined threshold of the ‘‘normal’’ behaviour of the system, and generate an alarm whenever it exceeds a predefined threshold. It will generate alarm while finding ‘‘abnormal’’ behavior of the system. The main differences between these methodologies are inherent in the concepts of ‘‘attack’’ and ‘‘anomaly’’. An attack can be defined as ‘‘a sequence of operations that puts the security of a system at risk’’. An anomaly is just ‘‘an event that is suspicious from the perspective of security’’. Signature-based system is used to detect specified, well-known attacks because it will be finding from signature database. Disadvanatage of this system is they are not capable of detecting new, unknown threats, even if they are built as minimum variants of already known attacks. On the other side, the main benefit of anomaly-based detection techniques is that they are able to detect previously unknown attacks.

On the basis of the analysis performed, intrusion detection systems are classified as either signature-based or anomaly-based.

Functionalities of IDS [11]

1. Monitoring and analyzing both user and system activities.
2. Analyzing system configurations and vulnerabilities.
3. Assessing system and file integrity.
4. Ability to recognize patterns typical of attacks.
5. Analysis of abnormal activity patterns.
6. Tracking user policy violations.

Threats [28][29]:

Intrusion causes availability , confidentiality , and integrity issues to cloud resources and services.

- Insider attack : Authorized cloud user may attempt to gain (and misuse) unauthorized privileges; insider may commit frauds and disclose information to others. This poses a serious trust issue.
- Flooding Attack : Attackers tries to flood victim by sending huge no. of packets can be of type TCP, UDP, ICMP or a mix of them. This attack may be possible due to illegimate network connections. It affects the service’s availability to authorized user
- User to Root Attacks: An attacker gets an access to legitimate user’s account by sniffing password . This makes him able to exploit vulnerabilities for gaining root level access to system
- Port Scanning : Port scanning provides list of open ports , closed ports and filtered ports. Throughout scanning , attacker can find open ports and attack on services running on these ports.
    - TCP Scanning
    - UDP Scanning
    - SYN Scanning
    - FIN Scanning
    - ACK Scanning
    - Window Scanning

- Attacks on Virtual Machine or hypervisor
  By compromising the lower layer hypervisor , attacker can gain control over installed VMs . Eg Bluepill, Subvirand DKDM are some well known attacks on virtual layer.
- Backdoor channel attacks
  It is passive attacks which allow hackers to gain remote access to the infected node in order to compromise user confidentiality .

II. RESEARCH METHODOLOGY

There are different techniques exist to perform intrusion detection some of them are the following.

2.1 Machine Learning Technique:

To make predictions and classification of intrusions, Machine learning algorithms build a mathematical model of sample data, known as "training data"[3].

Machine learning algorithms are used in different kinds of applications, such as detection of network intruders , email filtering, image processing and computer vision.

1]Artificial neural networks (ANNs)

Artificial neural networks (ANNs), builds upon the biological neural networks that constitute animal brains. The neural network is a framework for many different machine learning algorithms to work together and process complex data inputs. Such systems "learn" to perform tasks by considering examples, generally without being programmed with any task-specific rules[7].

2]Support vector machines (SVMs),

Support vector machines (SVMs), also known as support vector networks, are a set of related supervised learning methods used for classification and prediction[27]. It is supervised machine learning methos which contains a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm prepared a model that identify whether a intrusion falls into one category or the other.

3]Bayesian network

A Bayesian network, directed acyclic graphical model is also known as belief network is a probabilistic graphical model that represents a set of random variables and their conditional independence with a directed acyclic graph (DAG)[27].

4]Genetic algorithm (GA)

A genetic algorithm (GA) is a search algorithm and heuristic technique that imitate the process of natural selection, using methods such as mutation and crossover to generate new genotypes in the hope of finding good solutions to a given problem[27].

2.2 Deep Learning Technique :

Deep learning is part of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning technique can be supervised, semi-supervised or unsupervised[1].

Deep learning architectures such as deep neural networks, deep belief networks and recurrent neural networks have been applied to detect intrusions where they have produced results comparable to and in some cases superior to human experts. Deep Learning techniques are used in various fields including computer vision, speech recognition, natural language processing, audio recognition, social network filtering, machine translation, bioinformatics, drug design, medical image analysis, material inspection and board game programs[2].

1]Deep neural networks: A deep neural network (DNN) is an artificial neural network (ANN) which contains multiple layers between the input and output layers as compare with other Neural Network. The DNN finds the correct mathematical combinations to turn the input into the output, whether it be a linear relationship or a non-linear relationship. The network models find appropriate output by calculating probability moves through the layers.

2.Convolutional Neural Networks : Convolutional neural networks is also known as CNN or ConvNet . It is type of deep neural networks[2]. A CNN is trained by features with input data, and uses 2D convolutional layers, making this CNN model well suited to processing 2D data, such as attacks. One more advantage of CNN is, it eliminates the process of manual feature extraction, so you do not need to manually identify features from the data used to classify attacks. The CNN is used by extracting features directly from dataset. The relevant features are not pretrained; they are learned while the network trains on a collection of images. This automated feature extraction makes deep learning models highly accurate for computer vision tasks such as object classification.

3]Restricted Boltzmann Machines: In Boltzmann machine, each node is connected to every other node. Connection between all nodes are undirected. Boltzmann machine has not been proven useful for practical machine learning problems[3]. Boltzmann machine can be made efficient by placing certain restrictions. Restrictions like no intralayer connection in both visible layer and hidden layer. All visible nodes are connected to all the hidden nodes. RBM it has two layers, visible layer or input layer and hidden layer so it is also called as asymmetrical bipartite graph.

2.3 Evaluation Metrics for Intrusion Detection Systems

To evaluate Intrusion Detection Systems (IDSs) for their efficiency and effectiveness various features of the IDSs can be considered, like performance and correctness to usability.

The evaluation confusion matrix is used to represent classification results of the IDS.

Following are the factors for the measurement of IDS [7]

- Alarm: A signal, which suggest that a system has been or is being compromised.
- True Positive: A valid intrusion which triggers an IDS to produce an alarm (TP)
- False Positive: An event signaling an IDS to produce an alarm when no intrusion has taken place (FP).
- False Negative: IDS is not able to detect an actual intrusion(FN)
- True Negative: When no attack has taken place places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack

Confusion (Evaluation) matrix

Confusion matrix is a evaluation matrix that represents result of classification. It represents true and false classification results. The followings are the possibilities to classify events and depicted in Table 1 :

Table 1: Confusion matrix

Actual	**Predicted Attack**	**Predicted Normal**
Attack	TP	FN
Normal	FP	TN

Metrics from confusion matrix

Different performance metrics are defined in terms of the confusion matrix variables. These metrics generate some numeric values that are easily comparable.

1. Classification rate (CR): It is defined as the ratio of correctly classified instances and the total number of instances.

2. Detection rate (DR): It is computed as the ratio between the number of correctly detected attacks and the total number of attacks.

3. False positive rate (FPR): It is defined as the ratio between the number of normal instances detected as attack and the total number of normal instances.

4. Precision (PR): It is the fraction of data instances predicted as positive that are actually detected.

2.4 Datasets for Intrusion Detection System:

1. DARPA (Lincoln Laboratory 1998, 1999)[25]: This dataset was build for network security analysis purposes. DARPA contains tasks like send and receive files using FTP, send and receive email using SMTP and POP3, browse websites, log into remote computers using Telnet and perform work, send and receive IRC messages, and monitor the router remotely using SNMP.

Advantage : Attacks covers like DOS, guess password, buffer overflow, remote FTP, syn flood, Nmap, and rootkit.

Disadvantage : It is outdated for effective evaluation of IDS on modern networks in terms of attack types and network infrastructure. It does not shows real-world network traffic and contains irregularities such as the absence of false positives, and is outdated for the effective evaluation of IDSs.

2. KDD'99 (University of California, Irvine 1998, 99)[1][2][5]: The KDD Cup 1999 dataset was generated by processing the tcpdump portion of the 1998 DARPA dataset.
Advantage : KDD99 includes more than twenty attacks such as neptune-dos, pod-dos, smurf-dos, buffer-overflow, rootkit, satan, teardrop, etc.
Disadvantage: This dataset was created by merging network traffic and attack traffic in a simulated envionment, so their are large number of redundant records that are studded with data corruptions that leads to skewed testing results
3. DEFCON (The Shmoo Group, 2000)[26]: DEFCON-8 dataset was generated in 2000, contains port scanning and buffer overflow attacks, whereas the DEFCON-10 dataset which was created in 2002 uses port scan and sweeps, bad packets, administrative privilege, and FTP by telnet protocol attacks.
4. CAIDA (Center of Applied Internet Data Analysis – 2002/2016)[26]: CAIDA consists of three different types of datasets: Most of CAIDAs datasets are very specific to particular events or attacks and are anonymized with their payload, protocol information, and destination. 1) CAIDA OC48, which includes different types of data observed on an OC48 link in San Jose and provided by CAIDA members, DARPA, NSF, DHS, Cisco; 2) CAIDA DDOS attack dataset, which includes one-hour DDoS attack traffic split of 5-The attack classes present in the NSL KDD data set are grouped into four categories [5][9] :
1. DOS: Denial of service is an attack category, where it unable to handle legitimate requests by sending multiple request to system e.g. syn flooding
Relevant features: "source bytes" and "percentage of packets with errors"
2. Probing: This attack is used to watch and do the surveillance to gain information about the remote victim e.g. port scanning .
Relevant features: "duration of connection" and "source bytes"

3. U2R: This type of attack is also known as unauthorized access to local super user (root) privileges attack, by which an attacker tries to gain root/administrator access rights by exploiting some vulnerability in the victim using a normal account to login into a victim system and e.g. buffer overflow attacks.
Relevant features: "number of file creations" and "number of shell prompts invoked,"
4. R2L: The attacker attacks into a remote machine and gains local access of the victim machine by password guessing by unauthorized access from a remote machine

Relevant features: Network level features –"duration of connection" and "service requested" and host level features - "number of failed login attempts"minute pcap files; and 3) CAIDA Internet trace 2016, which is passive traffic traces from CAIDA's equinix-chicago monitor on High-speed Internet backbone..

5. CDX (United States Military Academy 2009)[25]: The CDX dataset shows how the network warfare competitions can be utilized to generate modern day labeled dataset. Nikto, Nessus, and WebScarab have been used by attackers to carry out probe and attacks automatically in this dataset.

6. Kyoto (Kyoto University – 2009)[25]: This dataset has been created using honeypots, so there is no process for manual labeling and anonymization, but it has limited view of the network traffic because only attacks directed at the honeypots can be observed. It has ten extra features such as IDS_Detection, Malware_Detection, and Ashula_Detection than the previous available datasets which are useful in NIDS analysis and evaluation.

7. Twente (University of Twente – 2009)[26]: To create this dataset, three services OpenSSH, Apache web server and Proftp using auth/ident on port 113 were installed to collect data from a honeypot network using netflow.

8. UMASS (University of Massachusetts – 2011)[26]: The dataset includes trace files which are network packets and some traces on wireless applications . It has been generated using a single TCP-based download request attack scenario.

9. CICIDS2017- Dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source and destination IPs, source and destination ports, protocols and attack (CSV files).

10. NSL-KDD DATASET NSL-KDD is a data set suggested to solve some of the inherent problems of the KDD'99 data set which are mentioned in [1][2][3].

The attack classes present in the NSL KDD data set are grouped into four categories [5][9] :
1. DOS: Denial of service is an attack category, where it unable to handle legitimate requests by sending multiple request to system e.g. syn flooding
Relevant features: "source bytes" and "percentage of packets with errors"
2. Probing: This attack is used to watch and do the surveillance to gain information about the remote victim e.g. port scanning .
Relevant features: "duration of connection" and "source bytes"
3. U2R: This type of attack is also known as unauthorized access to local super user (root) privileges attack, by which an attacker tries to gain root/administrator access rights by exploiting some vulnerability in the victim using a normal account to login into a victim system and e.g. buffer overflow attacks.
Relevant features: "number of file creations" and "number of shell prompts invoked,"
4. R2L: The attacker attacks into a remote machine and gains local access of the victim machine by password guessing by unauthorized access from a remote machine
Relevant features: Network level features –"duration of connection" and "service requested" and host level features - "number of failed login attempts"

Table 2. Datasets comparison with attacks

Dataset	Attack types						
	Browser Attack	**Bruteforce**	**DOS**	**SCAN**	**Backdoor**	**DNS**	**Other**
DARPA	Y	Y	Y	Y	N	N	Y
KDD99	Y	Y	Y	Y	N	N	Y
DEFCON	N	N	-	Y	N	N	Y
CAIDA	N	N	Y	Y	N	Y	Y
CDX	N	N	Y	Y	N	Y	-
Kyoto	N	Y	Y	Y	Y	Y	Y
Twente	N	Y	Y	Y	N	Y	Y
UMASS	N	N	-	Y	N	N	Y
CICIDS	Y	Y	Y	Y	Y	N	N
NSL KDD	Y	Y	Y	Y	Y	Y	Y

III. LITERATURE SURVEY

Nathan Shone, Tran Nguyen, Yu Dinh Phai, Qi Shi[1], proposed deep learning technique non-symmetric deep auto-encoder (NDAE) for unsupervised feature learning for intrusion detection, which addresses the feasibility and sustainability of current approaches. Furthermore, they also propose our novel deep learning classification model constructed using stacked NDAEs. This proposed classifier has been implemented in GPU-enabled TensorFlow and evaluated using the benchmark KDD Cup '99 and NSL-KDD datasets.

Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam[2], proposed a deep learning-based approach for developing such an efficient and flexible NIDS. They use Self-taught Learning (STL), a deep learning based technique, on NSL-KDD - a benchmark dataset for network intrusion.

Amjad Hussain Bhat, Sabyasachi Patra , Dr. Debasish Jena[3] , propose a anomaly Intrusion Detection System using machine learning approach using Naïve Bayes Tree (NB Tree) Classifier and hybrid approach of NB Tree and Random Forest for virtual machines on cloud computing. Their proposal is feature selection over events from Virtual Machine Monitor to detect anomaly in parallel to training the system so it will learn new threats and update the model. The experiment has been carried out on NSL-KDD'99 datasets.

Aryachandra AA, Fazmah Arif , Novian Anggis S[4] presented IDS server placement scenario for the successful detection and evaluate performance memory and CPU usage. They propose three types of placement IDS server. First, they place the IDS server inside the cloud server, the other scenario we place the IDS server separate from the cloud server, and the last they place IDS server both inside and separate cloud server. Within this paper they summarize that IDS server placement IDS depends on the major attacks

Yin Chuan-long, Zhu Yue-fei, Fei Jin-long, He Xin-zheng[5], propose a deep learning approach for intrusion detection using recurrent neural networks (RNN-IDS). Moreover, they study the performance of the model in binary classification and multiclass classification, and the number of neurons and different learning rate impacts on the performance of the proposed model. They compare it with those of J48, Artificial Neural Network, Random Forest, Support Vector Machine and other machine learning methods proposed by previous researchers on the benchmark dataset. The experimental results show that RNN-IDS is very suitable for modelling a classification model with high accuracy and that its performance is superior to that of traditional machine learning classification methods in both binary and multiclass classification. The RNN-IDS model improves the accuracy of the intrusion detection and provides a new research method for intrusion detection

Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande[7] proposed multi-threaded NIDS model for distributed cloud environment is based on three modules: capture & queuing module, analysis/ processing module and reporting module.

Claudio Mazzariello, Roberto Bifulco and Roberto Canonico[8], address the issue of detecting Denial of Service attacks performed by means of resources acquired on-demand. To this purpose, they propose to investigate the consequences of the use of a distributed strategy to detect and block attacks, or other malicious activities, originated by misbehaving customers of a Cloud Computing provider.

Yasir Mehmood, Umme Habiba[9], provides an overview of different intrusions in cloud. Then, they analyze some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect.

M.Kuzhalisai & G. Gayathri[10] has suggested AAA is a management module for authentication, authorization, and accounting. This was three way of checking , first checks the user's authentication information, if the user is authenticated, then AAA gets the user's anomaly level, which has been most recently generated, by inspecting the user's information in the database. According to the anomaly level it was deciding no of attacks to check.

Vikrant G. Deshmukh, Atul G. Borkut, Nikhil A. Agam[11] could detect various computer attacks by examining various attacker data record observed in processes on the network using Artificial Neural Networks (ANN) . They have implemented FC-ANN approach based on ANN and fuzzy clustering, to solve the problem.

Huang T. Zhu, Y. Bressan S. and Dobbie G[12] extend Local Outlier Factors to detect anomalies in time series and adapt to smooth environmental changes. And also propose Dimension Reasoning LOF(DR-LOF) that can point out the''mostanomalous'' dimension of the performance profile. DR-LOF provides clues for administrator stop in point and clear the anomalies.

Table 3: Literature Survey

Sr. No.	Ref	Type of IDS	Technique	Algorithm	Learning Technique	Dataset
1	[1]	Network based IDS	Deep learning	Auto Encoder	Unsupervised Learning	KDD Cup '99 and NSL-KDD
2	[2]	Network based IDS	Deep learning	Self-taught Learning (STL)	Unsupervised Learning	KDD Cup '99 and NSL-KDD
3	[3]	Host based IDS	Machine learning	NB tree algorithm and Random Forest classifiers	Supervised Learning	NSL-KDD'99
4	[5]	Network based	Deep learning	Recurrent Neural Networks	Unsupervised Learning	NSL-KDD
5	[6]	Network based	Deep learning	Restricted Boltzmann	Supervised	KDDcup 1999

				Machine (RBM)	Learning	
6	[8]	Network based	Machine Learning	Snort	Unsupervised	NSL KDD
7	[11]	Host based	Machine Learning	Artificial Neural Networks (ANN)	Unsupervised	KDDcup 1999
8	[12]	Host based	Machine Learning	WEKA Tools	Unsupervised	KDDcup 1999
9	[30]	Network based	Machine learning	Kernel Clustering	Unsupervised	KDDcup 1999
10	[31]	Network based	Machine learning	MLP - SVM 0 - NB - Logistic Random Forest Features Selection: BFS-CFS - GS-CFS	Supervised	Simulated Dataset
11	[32]	Network based	Swarm intelligence	FLN - PSO	Unsupervised	KDDcup 1999
12	[33]	Network based	Swarm intelligence	Binary PSO - k-NN	Unsupervised	KDDcup 1999
13	[34]	Network based	Machine learning	K-means - NB k-means - Information Gain	Unsupervised	NSL KDD 99
14	[35]	Network based	Machine learning	ANN – SVM	Unsupervised	UNB-CIC
15	[36]	Network based	Machine learning	Polynomial Feature Correlation	Unsupervised	KDD99

IV CONCLUSION

We discussed different dataset available and different techniques of an intrusion detection system that has been used to counter malicious attacks in the different environment. The study of various IDS architecture explained leads to a conclusion that Hybrid and Integrated IDS are best solution for network.

REFERENCES

[1] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, "A Deep Learning Approach for Network Intrusion Detection System" 9th EAI International Conference on Bio-inspired Information and Communications Technologies, At New Work, December2015

[2] Amjad Hussain Bhat , Sabyasachi Patra , Dr. Debasish Jena, "Machine Learning Approach for Intrusion Detection on Cloud Virtual Machines", International Journal of Application or Innovation in Engineering & Management, June 2013

[3] Aryachandra A A , Fazmah Arif Y , Novian Anggis S, "Intrusion Detection System (IDS) Server Placement Analysis in Cloud Computing" by Fourth International Conference on Information and Communication Technologies (IcoICT) 2016.

[4] Yin Chuan-long, Zhu Yue-fei, Fei Jin-long, He Xin-zheng, "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks" , IEEE 2017

[5] Khoi Khac Nguyen , Dinh Thai Hoang , Dusit Niyato , Ping Wang , Diep Nguyen , and Eryk Dutkiewicz, "Cyberattack detection in Mobile Cloud Computing : A Deep Learning Approach" WCNC 2018 conference

[6] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing" International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 .

[7] Yasir Mehmood, Umme Habiba, "Intrusion Detection System in Cloud Computing: Challenges and Opportunities" , 2nd National Conference on Information Assurance (NCIA) 2013

[8] M .Kuzhalisai & G. Gayathri "Enhanced Security In Cloud With Multi-Level Intrusion Detection System" International Journal of Computer & Communication Technology (IJCCT) ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012

[9] Vikrant G. Deshmukh, Atul G. Borkut, Nikhil A. Agam , "Intrusion Detection System For Cloud Computing" International Journal of Engineering Research & Technology (IJERT) 2013

[10] Huang T. Zhu, Y. Bressan S. and Dobbie G , "Anomaly detection and identification scheme for VM live migration in cloud infrastructure" Future Generation Computer System 2016

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

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

[13] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE transactions on dependable and secure computing, vol. 4, no. 1, pp. 1-15, 2007.

[14] P. Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", IEEE 2011 World Congress on Information and Communication Technologies, pp. 456-461, 2011.

[15] Yuebin Bai, Hidetsune Kobayashi, 2003. IntrusionDetection System: Technology &DevelopmentProceedings of the17th International Conference onAdvanced formation Networking and Applications(AINA'03).

[16] H. Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems ", Independent Study, September 2003.

[17] W. T Work, "Intrusion Detection Systems (IDS)", National Institute of Standers and Technology, 2003, available at: csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[18] What is intrusion detection? - Midmarket IT Security Definitions – Intrusion detection, http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.htmlAccessed on: 23/02/2012

[19] Jun-Ho-Lee,Min-Woo Park et.al " Multilevel Intrusion Detection System and Log Management in Cloud Computing" Feb 2012 at ICACT 2012

[20] M.Kuzhalisai & 2g.Gayathri "Enhanced Security In Cloud With Multi-Level Intrusion Detection System" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012

[21] Ring, Markus & Wunderlich, Sarah & Scheuring, Deniz & Landes, Dieter & Hotho, Andreas. (2019). A Survey of Network-based Intrusion Detection Data Sets.

[22] Brown, C., Cowperthwaite, A., Hijazi, A., and Somayaji,A. (2009). Analysis of the 1999 darpa/lincoln labora-tory ids evaluation data with netadhict. In2009 IEEESCISDA, pages 1–7.
[23] A. R. Vasudevan, E. Harshini, and S. Selvakumar, "SSENet-2011:A Network Intrusion Detection System dataset and its comparison with KDD CUP 99 dataset," in Second Asian Himalayas International Conference on Internet (AH-ICI), Nov 2011, pp. 1–5
[24] Shaikh A.A., Iyer K. (2019) Security and Privacy Issues in Cloud Computing. In: Hemanth J., Fernando X., Lafata P., Baig Z. (eds) International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018. ICICI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 26. Springer, Cham
[25] A. A. Shaikh. Attacks on cloud computing and its countermeasures. In2016 International Conferenceon Signal Processing, Communication, Power and Embedded System (SCOPES), pages 748–752, Oct2016.
[26] Di He, Xin Chen, Danping Zou, Ling Pei, and Lingge Jiang. 2018. An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection. 1–5. https://doi.org/10.1109/ISCAS.2018.8350994
[27] Jose Crispin Hernandez Hernandez, Béatrice Duval, and Jin-Kao Hao. 2007. A genetic embedded approach for gene selection and classification of microarray data. In European Conference on Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics. Springer, 90–101.
[28] MMohamad Nazrin Napiah, Mohd Yamani Idna Idris, Roziana Ramli, and Ismail Ahmedy. 2018. Compression Header Analyzer Intrusion Detection System (CHA-IDS) for 6LoWPAN Communication Protocol. IEEE Access 6 (2018), 16623–16638.
[29] Mohammed Hasan Ali, Bahaa Abbas Dawood AL Mohammed, Madya Alyani Binti Ismail, and Mohamad Fadli Zolkipli. 2018. A new intrusion detection system based on Fast Learning Network and Particle swarm optimization. IEEE Access 6 (2018), 20255–20261.
[30] Muna AL-Hawawreh, Nour Moustafa, and Elena Sitnikova. 2018. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications 41 (2018), 1–11. https://doi.org///doi.org/10.1016/j.jisa.2018.05.002 ID: 287016.
[31] Arief Rama Syarif and Windu Gata. 2017. Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. In Information and Communication Technology and System (ICTS), 2017 11th International Conference on. IEEE, 181–186.
[32] David Ahmad Effendy, Kusrini Kusrini, and Sudarmawan Sudarmawan. 2017. Classification of intrusion detection system (IDS) based on computer network. In Proceedings of 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE). IEEE, 90–94.