IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Brief Survey on Intrusion Detection System in Network Communication

M. Jeyakarthic[1*], A. Thirumalairaj[2]

[1]Department of Computer and Information Sciences, Annamalai University,Chidabaram, India
[2]Department of Computer Science, Kunthavai Naacchiyaar Govt Arts College for Women,Thanjavur, India

Corresponding Author: jeya_karthic@yahoo.com

Available online at: www.ijcseonline.org

***Abstract*—**Network Security is assuming an imperative job in a wide range of systems. These days the system is actualized in all spots like workplaces, schools, banks and so on and every one of the people are participating in informal community media. Despite the fact that numerous sorts of system security frameworks are being used, the helpless exercises are occurring occasionally. This research exhibits a study about different sorts of system attacks for the most part web attack, and distinctive Intrusion Detection System which are being used. This may clear a way to outline another sort of Intrusion Detection System which may shield the system framework from different kinds of system attack. Essentially Intrusion Detection Systems is been utilized based on two major methodologies first the acknowledgment of odd exercises as it by and large happens on the abandons normal or abnormal conduct and second abuse location by watching unapproved "marks" of those perceived vindictive attacks and grouping vulnerabilities. Oddity or the unknown (conduct based) Intrusion Detection Systems assume the distinction of ordinary conduct underneath assaults and accomplish anomalous exercises assessed and perceived with predefined framework or client conduct reference show. Our novel approach will mainly focus on detect the intrusion in network communication and provide a security.

***Keywords*—**Network security, Intrusion detection system, Classification

I. INTRODUCTION

A PCs organize is an arrangement of PCs associated together to share assets. A system attack can be executed by an insider or by an untouchable. In "Internal attack", the attack is started by a substance inside the security border, the individual who has finish approval includes in the powerless exercises, that is, the assailant attempts to get to some framework assets for which he isn't having the approval. It is extremely hard to discover this sort of people. An "External attack" is started all things considered, that is by an unapproved or ill-conceived client of the framework. In the Internet, the outside aggressors might be novice pranksters or sorted out culprits or global fear mongers or even unfriendly governments.

A PC arrange comprises of two parts to be specific equipment and programming. Both of these parts may have their very own dangers and vulnerabilities[4]. Equipment dangers are anything but difficult to recognize and furthermore it cause hurt just to the gadget as opposed to the information. The Hardware dangers are of four kinds: Physical, Electrical, Environmental and Maintenance. On the off chance that the attack is in programming, chiefly it hurts the information. Already, just the people with high programming aptitudes were engaged with composing of hacking programs. In any case, now, a man who has a little learning of programming may turn into a programmer just by downloading hacking instruments from the web. Next to this, everybody needs to utilize the high included programming for its drawing in highlights and it drives them to experience the attack effortlessly. Having high highlights is particularly inclined to need in the security. The three objectives of Software Security risk are Confidentiality, Integrity and Availability. The generally utilized system and which has countless is the Internet association. This web is nearly in every one of the fields. Despite the fact that the attack is in a wide range of systems, the most difficult one is the attack in Wide Area Network, that is the Web attack. System security is a territory where every single client needs his framework to be shielded from the gatecrashers[8]. As the interruption identification framework increments in number, comparably the Attack are additionally taking another birth or another shape. Knowing these vulnerabilities of the Intrusion Detection Systems, its points of interest and drawbacks definitely will plan and manufacture a system security framework. Thus it takes a shot at the system safe.

II. NETWORK ATTACKS

An attack can be an active or passive attack. In “Active attack”, the attacker will undergo some actions which may alter the system resources like breaking or bypassing the secured systems. Mostly it results in revealing sensitive information, modification of data or the maximum, loss of data completely. Trojan horses, viruses, worms, inserting malicious code, penetrating network data, stealing login information are some of the examples for the active attack. This type of attack is very harmful to the system. The types of active attacks are: Masquerade, Session Replay, Modification of message and Denial of service. A “Passive attack” tries to know or to use some important information but it does not affect the system resources. In this type of attack, the attackeruses some sniffer tool and waits to capture some sensitive information which can be applied for some other attacks. Traffic analysis software, packet sniffer tools, filtering the passwords are some of the passive attacks. The types of passive attacks are: Release message of contents and Traffic analysis.

The Attack might be either dynamic or aloof and it tends to be put under any of these four divisions. They are Denial of Service (DoS), Probing, Remote to User Attacks (R2L) and User to Root Attacks (U2R). DoS attack is a kind of attack in which the programmer or interloper makes the beneficiary framework occupied or it is by all accounts occupied, with the goal that he maintains a strategic distance from the sender machine to have a contact to the collector machine. Model: Apache, Smurf, Neptune, Ping of death, UDP storm and so on. Examining is an attack in which the programmer filters a machine or a systems administration gadget to discover its substantial IP address, the sort of administration, the working framework utilized and furthermore the shortcomings or vulnerabilities of the framework by utilizing hacking devices. These things might be utilized to misuse the framework in later date. Model: Saint, Portsweep, Mscan, Nmap and Ipsweep. In Remote to User Attacks, the aggressor who does not have a record on that machine sends some system bundles to an injured individual machine through the web, through which they make an association with that machine. At that point the aggressor makes harms the product of the machine and furthermore he may abuse the benefits of the first client of the machine. Precedents: Dictionary attack, and Password attack. In User to Root Attacks (U2R) attack, an assailant presents himself in the system as an ordinary client and in the wake of achieving some more secure zone he needs to go about as a super client by misusing the defenselessness present in PC instrument lastly he accomplishes the super client benefits. Here the aggressor is a piece of the system, so the recognizable proof of the assailant is extremely monotonous employment.

Eavesdropping Attack

An Eavesdropping Attack, which are otherwise called a sniffing or snooping assault, is an attack where somebody endeavors to take data that PCs, cell phones, or different gadgets transmit over a system.

Man-in-the-Middle Attack

In this the assailant makes free associations with the people in question and transfers messages among them and influencing them to trust that they are talking straightforwardly to one another over a private association, yet the truth of the matter is whole discussion is controlled by the aggressor.

DoS Attack

A denial-of-service attack or distributed denial-of-service attack is a push to make a PC asset out of stock to its Intended clients. In this kind of assault it back off the framework or close down the framework so it upset the administration and deny the authentic approved client. Because of this assault high system activity happens.

Intrusion detection

Intrusion can be characterized as the arrangement of activities that endeavor to trade off the classified amicability, uprightness or accessibility of a system resources that ponder unapproved access of the asset, they attempt to make an endeavor to:

1. Access the data
2. Deploying of information, or
3. Interpretation of data in a system to make defective or useless.

An intrusion detection system is a union of hardware and software components that detect harmful or malicious attempts in the network. Intrusion Detection Systems can screen all the system exercises and thus can distinguish the indications of interruptions. The basic purpose of Intrusion Detection Systems is to instruct the system regulator that any suspicious development happened.

There are two sorts of Intrusion identification systems: (A) Anomaly Detection: Recognize pernicious exercises dependent on deviations from the ordinary lead are considered as assaults. Despite the fact that it can distinguish obscure interruptions, the rate of missing report is low. (B) Misuse Detection: Recognize interruptions dependent on a standard example of the vindictive action. It very well may be exceptionally useful for known assault designs. Likewise, the rate of lost report is high. One weakness of Misuse Detection over Irregularity Detection is that it can just notice interruptions which contain known examples of assault. An Intrusion Detection Systems screens the exercises of a given domain and chooses whether these exercises are malevolent or typical dependent on framework respectability, privacy and the accessibility of data assets.

When building Intrusion Detection Systems one needs to think about numerous issues, for example, information gathering, information preprocessing, interruption acknowledgment, detailing, and reaction.

III. Related Work

In 2017, it is important to distinguish these assaults right on time to ensure end-clients and also the system foundation assets. The center of this work is to execute the Intrusion identification framework or, in other words the Internet specialist organizations level. Utilizing our self-created reproduction programming, it will be demonstrated that how ISPs shape the insurance rings around the host to team up and safeguard the movement data. DDoS can close down an association for a considerable length of time – or even days henceforth making it troublesome for associations to reestablish back to its place. At this moment, the issue in this day and age is the expansion in development of Cyber-assaults exponentially making it more troublesome and hard to distinguish the requirement for a superior Intrusion Detection System. The issue additionally happens with current Intrusion Detection System's which creates high rate of false alerts. Our principle objective is to make a model reproduction demonstrating the assaults occur at the ISP level utilizing the system hubs. We also demonstrate an ongoing assault where a live exhibit of assault being occurring will be appeared for simple comprehension in this field on Cyber Security. It demonstrates to enhance the execution of assault identification programming's as far as exactness and to diminish the abuse of exploited people from the assaults.

In 2017 Intrusion Detection Systems, information mining strategies is comprehensively utilized for removing helpful data from the gigantic sum dataset. This research introduces the examination of various systems and interruption arrangement on KDD Cup 99 dataset. In this way, by arranging the distinctive system issues another and viable method is actualized which can classify and recognize interruptions in the KDD Cup 99 dataset. The target of the Intrusion Detection Systems is the controlling state and dynamic conduct of the PC framework. This recognition framework checks every one of the exercises of investigated bundles on a system. Intrusion Detection Systems perceive what assets are being used and which program gets to those assets. In the event that in the system any variations or change occurs, framework direct get some system alarms. Intrusion Detection Systems is dynamically getting to be fundamental to guarantee the host PC systems and its system exercises. Intrusion Detection Systems with host based data is fused into the PC structures to recognize the gatecrasher unusual exercises, poisonous Behavior, application variations from the norm and protect the Information Systems from interlopers and report the events to the Intrusion Detection Systems System Administrator. In the wake of looking over the different Anomaly based Intrusion Detection Systems strategy inferred that solitary system can't give precise recognition rate. For boosting the irregularity identification strategy, an effective programmed half and half procedure is proposed to accomplish exact recognition rate. Likewise, diminishes the false expectation rate and in addition diminish the time many-sided quality. Furthermore, machine learning systems diminish the system movement.

In 2016, to stay away from the quick sending procedure utilized by hurrying and wormhole hubs, we utilize a measurable oddity based strategy. The thought is to empower group head hubs to recognize that noxious hub has a high limit of rivalry in course choice. The objective is to choose courses that don't go through stacked group hubs which have high determination rates. This methodology recognize vindictive hub as well as adjusts stack by disposing of activity focus focuses from the system. Anyway an authentic hub might be set at a key area of network in the bunch, and consequently can be identified as malignant hub in light of its high course determination rate. To keep away from this issue our recognition strategy considers the system portability. Since, despite the fact that a real hub might be put at a key area of availability in the bunch, it would not remain in a similar area for long, as the system topology is dynamic. In this manner dependent on the evaluated portability we can decide whether the high node's determination rate is because of its vital position and low versatility, or because of its vindictive conduct.

In 2016 mAIS model, a non-self identifier set is prepared utilizing Negative Selection to distinguish self and recognize non-self. A second identifier set is prepared to distinguish non-self and identify self. The second finder set is alluded to as the self locator set. These two finder sets are utilized in a Proportion Based Classification technique (see beneath) to distinguish and identify new cases. The two locator sets are utilized in an extent based order technique to recognize obscure cases. On the off chance that the extent of non-self develop identifiers that match an occurrence is more noteworthy than the extent of self develop indicators that match the occasion, the example is delegated non-self. Similarly, if the extents of self develop identifiers that match are more prominent than the extent of nonself develop finders, the occasion is delegated self. Since, false negatives (FNs) can possibly cause altogether more harm than those of false positives (FPs), in the uncommon case that the extents of the two free identifier sets are equivalent, the occurrence is named non-self. An expansion in the number and decent variety of starting identifiers merits investigating. A bigger number of starting identifiers and an enhanced arrangement of general and particular finders would give the mAIS and AIS more noteworthy inclusion of the speculation space and also giving better acknowledgment of self and non-self.

In 2016, proposed system incorporates both inward and additionally outer interruption recognition instruments. Framework contains two calculations to distinguish interruption. Framework distinguishes both inside and also outer assaults, in coordinated way. In proposed framework, when different PCs are appended to one another, every framework has its inward interruption identification component and for outside interruption location FGA is utilized. In inside interruption identification framework, signature coordinating calculation is utilized. At the point when client fires inquiry on database, it is checked utilizing calculation. In preparing of calculation, terminated inquiry is contrasted and put away marks of vindictive questions. In the event that similitude file surpasses characterized edge then it is named strange question and notice is given to administrator to take additionally activities. Distinctive procedures, for example, Neural Network, Clustering, Genetic calculations are available to identify interruption. Here and there approved clients of framework do interruption for pernicious reason. The previously mentioned assaults are difficult to distinguish. Mark coordinating calculation is utilized to identify inward interruption. Fuzzy hereditary calculation is utilized to recognize malignant parcels in outer assault identification. The proposed framework distinguishes inward and outside aggressors in incorporated route in a solitary framework and square them.

In 2014, proposed work utilizes the mix of abnormality based interruption identification utilizing to identify any irregularity in the system and after that to diminish the false positives got, the perceptions from just the confided in hubs are considered. The trust calculation system utilizes Dempster-Shafer hypothesis which is a dubious learning strategy for social occasion conviction estimation of a hub from different hubs in the system. The classifier is prepared utilizing the known system design with both assault and non-assault designs. This uses the Euclidean separation measure to acquire the comparability between the examples. The test dataset contains no class mark, thus dependent on the preparation the class names are doled out for the examples. It bunches comparative information cases into a few dimensional cross section. The SOM classifier finds the best coordinating unit for the test informational index therefore, can be bunched in gatherings with comparable highlights. As abnormality based interruption discovery systems depend on factual information they can result in false positive distinguishing proof of ostensible example as an assault. This bogus recognizable proof of favorable conduct as irregular can result in detachment of non-pernicious hub as vindictive, along these lines may bring about apportioning of the system. In this manner, with the end goal to enhance the precision of the oddity based interruption recognition framework the trust estimation of the hubs assumes an essential job. Acquiring the trust estimation of the hubs and after that getting to the examples created from profoundly confided in hub can give exact distinguishing proof of interruption. In this manner, false positives got from utilizing oddity based interruption location alone can be lessened when consolidating both the strategy.

In 2014, an intrusion detection system continuously has a center component - a sensor which is in charge of recognizing interruptions. The sensors dependably get crude information data sources. An occasion generator is in charge of information accumulation. Occasion generator has its known approach that characterizes the separating method of occasion warning data. The analyzer (sensor) channels data and disposes of any superfluous information got from the arrangement of occasions related with the secured framework, accordingly recognizing suspicious exercises. The analyzer utilizes the recognition arrangement database for this reason. The last contains the accompanying components: assault marks, ordinary conduct profiles, important parameters (for instance, limits). Furthermore, the database holds Intrusion Detection Systems setup parameters, incorporating methods of correspondence with the reaction module. Dispatcher; as indicated by its approach circulates the information movement to the analyzers. This, could influence on location time and exactness. Equalizer; requires in host web application information, which bolsters information standardization. Connection motor; dependable to decrease the aggregate number of alarms and messages that should be seen by the framework head to as few as conceivable by combining comparative occasions into gatherings.

IV. METHODOLOGIES

Naive Bayes

Naive Bayes can perform exceptionally well when moderate conditions exist in the information. It has been demonstrated that the execution of Naïve Bayes classifier enhances when excess highlights are evacuated. An experimental examination on the KDD Cup '99 informational collection, looking at the execution of Naive Bayes and a Decision Tree. The Decision Tree got a higher precision, yet NB acquired better discovery rates. A proposed structure of system interruption recognition framework dependent on information mining calculation, Naïve Bayes. The examinations were directed on 10% of the KDD99 dataset and 10-overlap cross approval was utilized for assessment. The outcomes demonstrated that the recognition rate was 95%, with a mistake rate of 5%. In addition, it performed quicker (1.89 seconds) to assemble the model, proficient and practical.

.Decision trees

Decision trees are well known in abuse identification frameworks, as they yield great execution and offer a few advantages over other machine learning strategies. The

Decision tree gotten great exactness, however does not execute and in addition different procedures on a few classes of interruption, especially User to Root and Remote to User assaults, the two of which are minor classes and incorporate a substantial extent of new assault types. Besides, they discovered that Decision tree and Random Forests (troupe of Decision tree) are exceptionally delicate to the information chose for prepring, i.e., the execution fluctuated altogether on various folds (subsets) of the information.

A Decision tree made out of three fundamental components:

- A Decision node exhibiting test or condition on information thing.
- An edge or a branch which compares to the one of the conceivable quality which implies one of the test variable results.
- A leaf which decides the class to which the protest has a place.

Support Vector Machine

Support vector Machine (SVM), another promising example arrangement system, a compelling Classification strategy and directed learning calculations, which have been connected progressively to abuse location in the most recent decade. SVM as a parallel classifier calculation that searches for an ideal hyper plane as a choice capacity in a high dimensional space and Figure 4 demonstrates the SVM edges and bolster vectors. Besides, they are prepared immediately contrasted and MLPs. SVM and bit strategies are the mainstream apparatuses for information mining assignments, for example, characterization, relapse and curiosity discovery. Neural Networks (NN) and Support Vector Machine for intrusion detection framework. The two primary explanations behind utilizing SVM for interruption identification are: speed and adaptability. The trials were done utilizing DARPA 1998 dataset. SVM IDS was produced by performing preparing and testing on the dataset. The prepared set accomplished a runtime of 17.77 seconds and testing set got 99.50% exactness with a runtime of 1.63 seconds. The execution of SVM demonstrated that SVM IDS have marginally higher rate of making the right identification.

K-nearest neighbors

K-closest neighbors (K-NN) order is connected to the information where the earlier learning of information is missing or to perform segregate examination when dependable parametric assessments of likelihood densities are obscure or hard to decide. For grouping K-NN needs the preparation information to outline test information in the element space. In this, for given k, that is no. of neighbors to be considered, K-NN positions the neighbors of a test vector T among the preparation tests, and uses the class marks of the k most closestneighbors to foresee the class of the test vector. Euclidean separation is typically utilized for estimating the comparability between two vectors.

V. PROPOSED WORK

Intrusion detection Systems are intended to system frameworks from different system attack and viruses. IDSs are intended to safeguard PC frameworks from different system attack and viruses. IDSs fabricate successful order models or examples to recognize ordinary practices from anomalous practices that are spoken to by system information. To arrange organize exercises (in the system log) as ordinary or unusual while limiting misclassification. To shield system frameworks from different system attack and system viruses.

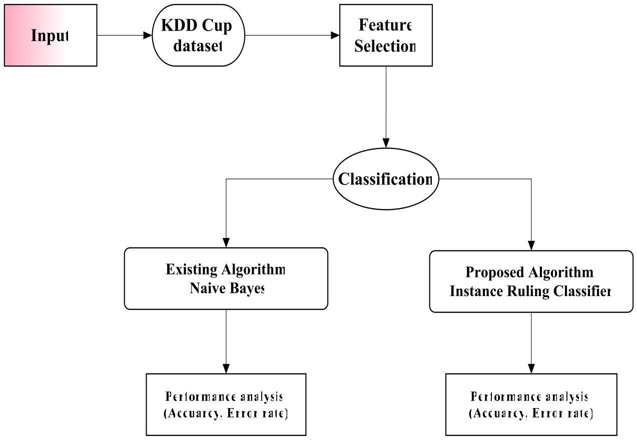
Input
KDD Cup dataset
Feature Selection
Classification
Existing Algorithm Naive Bayes
Proposed Algorithm Instance Ruling Classifier
Performance analysis (Accuarcy, Error rate)
Performance analysis (Accuarcy, Error rate)

Figure 1. Instance ruling classifier framework

To adjust the execution of IDS as far as productivity and precision. IDSs are design to guard PC frameworks from different digital assaults and PC viruses. In instance ruling classifier algorithm for classification of new thing, it first needs to make a choice tree dependent on the quality estimations of the accessible preparing information. It segregates the different occasions and recognizes the property for the equivalent. This element that can reveal to us most about the information examples with the goal that can characterize them the best is said to have the most elevated data gain. I will expect the 81.5% of correctly classified instance using Instance Ruling Classifier.

1. Instance Ruling Classifier models to recognize ordinary performance from irregular performances that are spoken to by system information.
2. To arrange organize exercises (in the system log) as ordinary or unusual while limiting misclassification. To shield PC frameworks from different digital assaults and PC infections.
3. To adjust the execution of IDS regarding proficiency and exactness.

VI. CONCLUSION

According to the concentrated of systems recommended by different researchers, the manners in which it can identify the interloper are introduced here. A Survey from incorporates high false positive rate, yet our framework decreases the false positive rate nearly. One of the overviews from proposes that there are preparing delays in expansive size of system there in our framework, the interlopers are distinguished progressively and furthermore gives a rundown of gatecrashers and their exercises and relatively to the review, it is less tedious, So, when planning another intrusion detection system, these qualities can be utilized continuously framework to recognize the inside interlopers and their malignant practices. This will be a legitimate intrusion detection system which will distinguish the interior interloper's precisely continuously and can be utilized by a few firms, MNC's for ensuring their important information.

REFERENCES

[1] C Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing” www.ietf.org-RFC3561, 2003, pp 01-31.

[2] Dr. S. Vijayarani & Ms. Maria S.S., “Intrusion Detection System- A Study”, IJSPTM Vol4, No1, February 2015, pp 31-44.

[3] Ehsan Amiri, Hassan K, H Heidari, E. Mohamadi, Hossein M., “Intrusion Detection System in MANET: A Review”, Procedia- Social and Behavioral Sciences 129(2014), ELSEVIER, ScienceDirect, pp 453-459.

[4] Ming-Yang Su, Gwo-Jong, YuChun-Yuen Lin, “A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach” Computer & Security, ElLSEVIER, Volume 28, Issue 5, July 2009, Pages 301–309.

[5] Roman Fekolkin, “Intrusion Detection & Prevention System: Overview of Snort & Suricata” Internet Security, A7011N, Lulea University of Technology, Jan 06, 2015 pp 1-4.

[6] S. Mukkamala, G. Janoski, and A. Sung “Intrusion detection using neural networks and support vector machines,” International Joint Conference on Neural Networks (IJCNN). vol. 2: IEEE, 2002, pp. 1702- 1707.

[7] Ved Prakash Mishra & Balvinder Shukla, “Process Mining in Intrusion Detection – The need of current digital world”, Springer Nature Singapore Pte Ltd. 2017: CCIS 712, pp. 238–246, 2017.

[8] R. Fekolkin, “Intrusion Detection & Prevention System: Overview of Snort & Suricata, Internet Security”, A7011N, Lulea University of Technology, Jan 06, 2015 pp 1-4.

[9] Md. Mostaque & M Hassan, “Current studies on Intrusion Detection System”, Genetic algorithm and Fuzzy logic, International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2.2013 pp. 35 -47.

[10] R.P.J.C Bose, W.M. P Van der Aalst, I, Žliobait˙e, & M Pechenizkiy, “Dealing with Concept Drifts in Process Mining”, IEEE Transactions on Neural Networks and Learning Systems, Vol. 25, No. 1, 2014 pp. 154 – 171.

[11] M.Y. Su, G Jong, Y Chun, & Y Lin, “A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach”, Computer & Security, ELSEVIER, Volume 28, Issue 5, 2009, pp 301–309.

[12] V P Mishra, Yogesh Waran, Subheshree, “Detecting Attacks Using Big Data with Process Mining”, International Journal of System Modeling and Simulation, v. 2, n. 2, June 2017, p. 5-7.

[13] Hussein, Safwan Mawlood, Fakariah Hani Mohd Ali, and Zolidah Kasiran. “Evaluation effectiveness of hybrid IDS using snort with naïve Bayes to detect attacks.” Digital Information and Communication Technology and it's Applications (DiCTA?). 2012 Second international Conference on. IEEE, 2012.

[14] Marin, Jack, Daniel Ragsdale, and 1. Sirdu. “A hybrid approach to the profile creation and intrusion detection.” DARPA information Survivability Conference &amp; Exposition ii, 2001.

[15] Aydin, M. Ali, A. Halim Zaim, and K. Gokhan Ceylan. “A hybrid intrusion detection system design for computer network security.” Computers & Electrical Engineering 35.3 (2009): 517-526.

[16] Arnza, Cristina, Catalin Leordeanu, and Valentin Cristea. "Hybrid network intrusion detection." Intelligent Computer Communication and Processing (ICCP), 2011 iEEE International Conference on. IEEE, 2011.

[17] Northcutt, Stephen. Snort: IDS and IPS toolkit. Eds. Jay Beale, and Toby Kohlenberg. Syngress Press, 2007.

[18] AI-mamory, Safaa, and Firas S. Jassim. "Evaluation of Different Data Mining Algorithms with KDD CUP 99 Data Set." Journal of Babylon University/Pure and Applied Sciences 21.8 (2013): 2663-2681.

[19] Shanmugavadivu, R., and N. Nagarajan. "Network intrusion detection system using fuzzy logic." Indian Journal of Computer Science and Engineering (JJCSE) 2.1 (2011): 10 I-Ill.

[20] Hochberg, Judith, et al. "NADIR: An automated system for detecting network intrusion and misuse." Computers & Security 12.3 (1993): 235- 248.

[21] Teng, Shaohua, et al. "A cooperative network intrusion detection based on fuzzy SVMs." Journal of Networks 5.4 (2010): 475-483.

[22] Mining, Data, I. Han, and M. Kamber. "Data mining concepts and techniques." Morgan Kaujinann (2006).

[23] IIgun, Koral, Richard A. Kemmerer, and Phillip A. Porras. "State transition analysis: A rule-based intrusion detection approach." iEEE transactions on software engineering 21.3 (1995): 181-199.

IIgun, Koral. "USTAT: A real-time intrusion detection system for UNIX." Research in Security and Privacy, 1993. Proceedings. , 1993 IEEE Computer Society Symposium on. IEEE, 1993.