Security Issues in Intrusion Detection – Review

Dr. Rakoth Kandan Sambandam
Dr.S. Thaiyalnayaki
Dr. S.K. Aruna
Mr. N. PrabuSankar

1 & 3 Assistant Professor, Dept. of Computer Science and Engineering, School of Engineering and Technology, CHRIST (Deemed to be University) – Kengeri Campus, Bangalore, Karnataka, India.

2 Associate Professor, Dept. of Computer Science and Engineering, School of Computing, Bharath Institute of Higher Education and Research (Deemed to be University), Chennai, Tamilnadu, India.

4 Assistant Professor, Dept. of Computer Science and Engineering, School of Computing, Bharath Institute of Higher Education and Research (Deemed to be University), Chennai, Tamilnadu, India.

E-mail: ID - rakoth.kandan@christuniversity.in*

Article Info
Page Number: 47-58
Publication Issue:
Vol 71 No. 3s2 (2022)

Abstract

Network information security is what computer network security is all about. It alludes to the organizational framework that we utilize to shield data stream and information from coincidental harm, spills, and different issues. The privacy, truth, correctness, and safety of computer networks are all directly related to network security. Due to a variety of security threats and hazards, an organization's critical data is at risk. Intrusion is one sort of risk that involves attempting to circumvent the computer system's normal security safeguards. ID is a means of identifying security breaches in a computer network by checking and evaluating the activities that are issued. IDS play a critical role in ensuring the security of a network. This paper gives a broad overview of computer network security and intrusion detection systems, allowing anyone who reads it to get a basic understanding. This paper also provides a basic overview of network security and intrusion detection system assaults.

Article History
Article Received: 28 April 2022
Revised: 15 May 2022
Accepted: 20 June 2022
Publication: 21 July 2022

Keywords: - Intrusion, Security, Risk, Network’s

1. Introduction

The internet has evolved into a universal means of communication for a vast number of companies as network technology continues to advance. As a result of this massive growth, many organizations are encountering a slew of challenges in storing their critical data and information in the network on a daily basis [1]. Many networks have apparently been subjected to a slew of attacks. One type of attack is intrusion.

It is a legitimate demonstration to use information and PC assets without a permit, bringing about quick injury and a security break. Interruption discovery is the act of observing and examining what is happening in a PC or organization to identify security breaks. Intrusion Detection Systems analyze network traffic and identify acts that violate personal computer and network security policies. It also educates the public about the system.

The presentation of firewalls, switches, servers, and basic records is additionally inspected by the Intrusion Detection System. However the essential objective of an interruption recognition framework is to identify interruptions, it is additionally needed to offer types of assistance like reviewing framework setup and weaknesses, assessing organization, equipment, and record respectability, following deviation, noticing and dissecting organization and framework conduct, and giving an easy to understand limit to security organization.

2. NETWORK SECURITY TECHNOLOGIES

2.1. Firewall

Firewall innovation is an assortment of security includes that permit clients to acquire constrained admittance to an outside network by using foreordained wellbeing highlights across network frameworks. Information move between at least two organizations should cling to specific wellbeing measures to survey execution, decide if correspondence between the organizations is admissible, and monitor the organization's status.

2.2. Data Encryption

Information encryption innovation is separated into five classifications: information stockpiling, information travel, information respectability, confirmation, and key administration. To forestall information misfortune and deconstruction, encryption is put away in memory. During the transmission cycle, circuit encryption and port encryption are regularly utilized to encode information. Information uprightness recognizable proof innovation ensures data travel, extra room, access, character, and mystery among individuals, just as information utilization [2]. The boundary esteem choice on whether the information matches the set worth describes the framework in this technique. Confirmation of information is required, and encryption has further developed security. For information encryption in Key administration is assuming a significant part as a rule. Key administration strategies incorporate key age, circulation, stockpiling, and obliteration.

2.3. Anti-Virus

Against infection, innovation incorporates something beyond hostile to infection programming. It can likewise be separated into two kinds: network hostile to infection programming and independent enemy of infection programming. Aside from contaminations, the online enemy of infection programming centers around network associations [3]. When the infection has tainted the organization, it will be quickly found and dispensed with by online infection programming.

THREATS IN COMPUTER NETWORKS

Virus and Features.

PC networks permit individuals to move and trade information, yet they additionally permit PC infections to spread and jeopardize individuals' security and protection. Consistently, many infections are found and dispersed rapidly by web programmers with the end goal of information hacking and getting into others' security. A PC infection is a program equipped for self-imitating and causing fluctuating levels of annihilation. Users are unable to detect the reproduction of these infections since the data is masked by commonly used files. When users access this data or files, the virus replicates and spreads [4]. A first-generation computer virus falls into this category. There is a new strain of the virus that does not require any data concealing. It hides in the network and causes problems for malicious program users. It makes use of web media, grows quickly, and causes a wide range of problems.

Threats of hackers.

Computer networks enable individuals to share and exchange data, but they also allow computer viruses to proliferate, putting people's security and privacy at risk. Every day, online hackers find and immediately disseminate dozens of viruses with the intent of data hacking and prying into other people's personal information. A computer virus is a programme that may replicate itself and cause varied degrees of damage. Because the data is camouflaged by regularly used files, users are unable to identify the reproduction of these infections. The virus replicates and spreads when users access this data or files [4]. This is the place where an original PC infection fits in. Another strain of the infection has arisen that doesn't need information disguise. It stows away in the organization, creating issues for clients of pernicious projects. It makes the benefit of electronic media, spreads quickly, and produces an assortment of issues.

4. STEPS TO ENHANCE NETWORK SECURITY

4.1. Ways to Measure Online Anti-Virus.

Computer networks enable individuals to share and exchange data, but they also allow computer viruses to proliferate, putting people's security and privacy at risk. Every day, online hackers find and immediately disseminate dozens of viruses with the intent of data hacking and prying into other people's personal information. A computer virus is a program that may replicate itself and cause varying degrees of damage. Because the data is camouflaged by regularly used files, users are unable to identify the reproduction of these infections. The virus replicates and spreads when users access this data or files [4]. A first-generation computer virus falls into this category. There is a new strain of the virus that does not require any data concealing. It stows away in the organization, bringing on some issues for clients of malignant projects. It exploits online media, spreads quickly, and produces an assortment of issues.

4.2. Measure to Prevent Hackers.

Subjective security issues and objective security issues are the two types of breaches and attacks. Subjectivity security issues allude to botches made by network the board staff, though objectivity security issues allude to blemishes in PCs and organizations that programmers exploit to complete different sorts of assaults.

4.3. Safety Tool Usage

The previously mentioned essential techniques for PC network security can be utilized to gather have PC security issues. Network the executives experts effectively distinguish these issues and introduce the fix [7]. Network overseers utilize examining programs (like NAL's CyberCop Scanner) to filter have frameworks, recognize points of failure, and take proper preventive and fix measures.

4.4. Firewall Technology

Firewall innovation goes about as a safeguard to keep others from accessing your organization gadget. Parcel separating innovation, specialist innovation, and status checking innovation are the three classifications of firewall advancements. By designing the web convention address, bundle separating innovation demonstrates it. A firewall will be utilized to channel tends to that don't match the design. This is the principal line of guard. The second kind of innovation is specialist innovation, which is utilized to check the power of solicitations presented by an intermediary server's permitting customer. This technique additionally covers the inner machine addresses and incorporates affirmation, login, and essential sifting measures. The third era of organization security advances is the Status observing innovation, which is compelling at all phases of organization checking. It improves the probability of settling on brief security choices. This innovation proficiently secures the nearby organization against programmer interruption and ensures the whole organization.

4.5. Switch Measurement

When assembling an enormous scope local PC organization, we should ensure that the switch is associated with an organization, which may be a solitary organization, so the switch can shape its own administration network [8]. Therefore, the general number of organization switches will be limited, just as the potential for frustration. Network supervisors can likewise utilize the chase and find to rapidly manage remote organization deficiencies.

5. INTRUSION DETECTION

The reason for interruption identification innovation is to guarantee the security of plan and assignment. It can rapidly distinguish framework imperfections and the approved situation in a report. It can distinguish and address framework weaknesses without wasting any time. Routinely, advances that are disregarding security approaches are utilized.

5.1. Types of Intrusion Detection System

Interruption identification frameworks are separated into two sorts: have based interruption recognition frameworks and organization based interruption discovery frameworks. A host-based IDS secures the whole framework. Specialists are accustomed to global positioning framework exercises, for example, framework dependability, application activities, network traffic, document process, record variety, and working framework exercises, with a log document being made to monitor everything. In the event that any unapproved passage, adjustment, or action is recognized, the host-based IDS cautions the framework by means of spring up notices, hinders the action, and tells the administration server [9]. The sort of safety rule carried out by the nearby framework chooses whether or not the interruption ought to be recognized, hindered, or cautioned. This kind of interruption recognition framework is introduced on a solitary host.

An organization based interruption identification framework watches out for the organization to forestall unapproved section. The activities of the association are endorsed in a log archive, which is used by IDS to recognize risks and anomalies. Network-based IDS identifies interruptions, for example, DOS and root attacks. All organization traffic enters and exits through an organization based IDS framework [10]. Network-based IDS screens all organization traffic and is carried out at the organization's edge or on an organization fragment. It examinations traffic and actually takes a look at bundles progressively to identify interruptions. Dynamic parts allude to arrange based IDS methodology, though latent parts allude to have based IDS strategies. A crossover interruption location framework, which consolidates network-based and have based IDS, is presently utilized in many organization settings. It gives you more opportunity and security.

5.2. Anomaly Detection

This component stores network bundle data, an application running data, framework long activities, working framework data, and part data. On the off chance that the previously mentioned boundaries dissent, the irregularity is identified and caution is created. Anomaly detection can help with anomaly detection, network-based intrusion detection, and other strange system events [11]. It detects a system breach based on typical activity and is also known as actions-based recognition. This method is capable of detecting new and unreported threats by analyzing review data. This methodology, nonetheless, has a high pace of bogus cautions.

5.3. Misuse Detection

This approach preserves the pattern layout, attack signatures, and intrusion patterns in the database. The system's behaviors are compared to intelligence that has been previously stored. The alert is triggered if a match is found. This approach is known as signature-based recognition since it compares signatures. To protect against new sorts of attacks, these strategies update their databases automatically based on varied input data [12]. When it comes to locating recognized assaults and their alternatives, misuse detection systems are quite precise. These systems, however, are unable to detect unknown invasions because they rely on fingerprints.

5.4. Target Monitoring

This strategy searches for irregularities in exact documents and revises them. It fills in as a disciplinary control that reestablishes a record later it has been altered by a gatecrasher. Cryptographic disarray figuring is utilized to recuperate the tweaked substance. Because the administrator does not need to constantly monitor traffic, this system is straightforward to implement. When a data checksum difference is detected, an alarm is delivered to the network or system. The calculation of the checksum can be timed at various intervals.

5.5. Secrecy Inquiries

This strategy identifies interlopers who stay in the organization for a lengthy timeframe. Commonly, aggressors check for framework weakness and open ports for a lengthy timeframe prior to dispatching an attack [13]. A total wide assortment of information about the whole framework is utilized to check for any such deliberate assaults. . To find assaults requires an enormous number of tests, which are typically gathered from various gadgets and organizations. It achieves this by consolidating peculiarity identification and misuse finding.

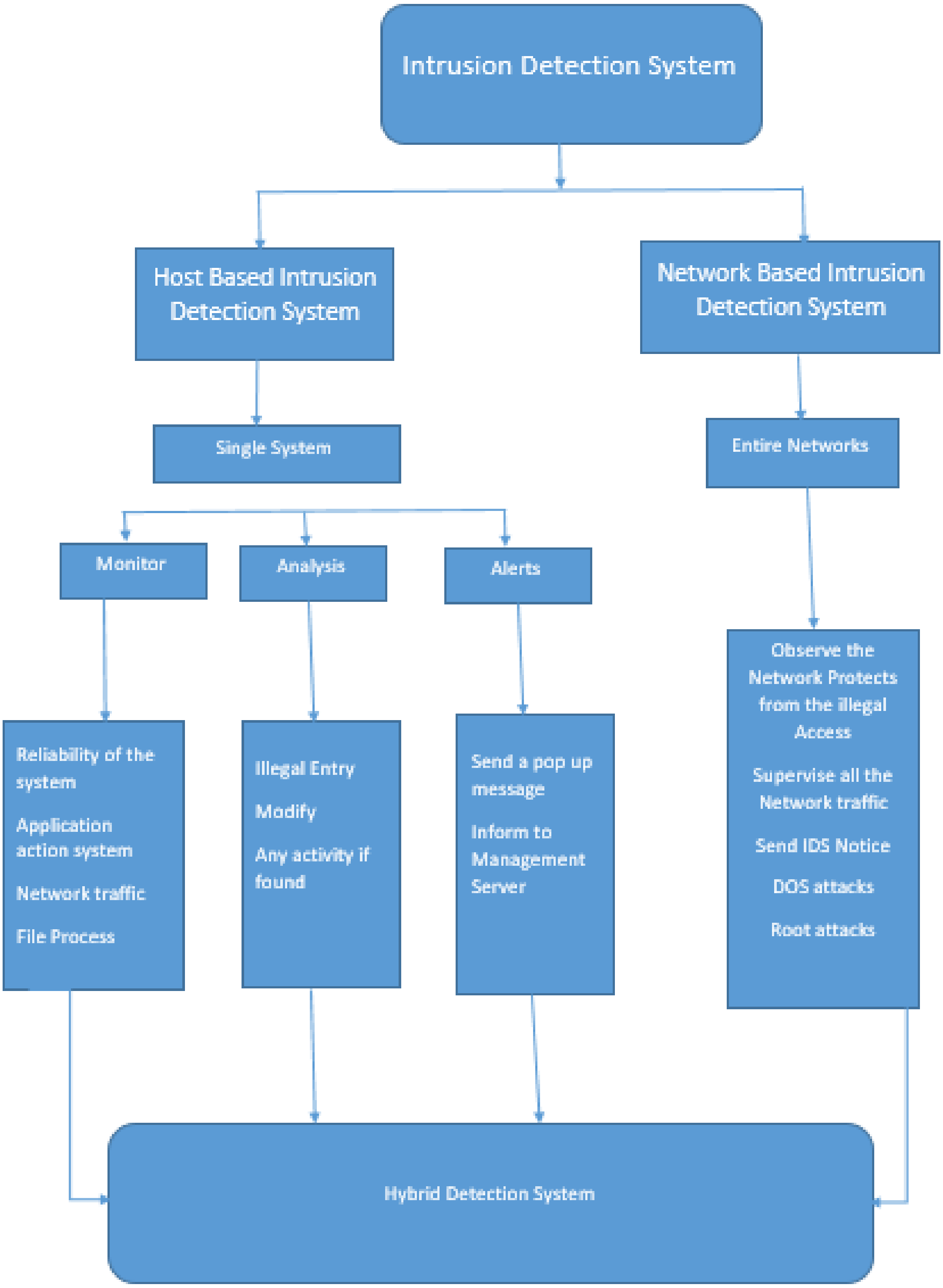
Intrusion Detection System
Host Based Intrusion Detection System
Network Based Intrusion Detection System
Single System
Entire Networks
Monitor
Analysis
Alerts
Reliability of the system
Application action system
Network traffic
File Process
Illegal Entry
Modify
Any activity if found
Send a pop up message
Inform to Management Server
Observe the Network Protects from the illegal Access
Supervise all the Network traffic
Send IDS Notice
DOS attacks
Root attacks
Hybrid Detection System

Figure 1. Architecture Diagram Figure

6. ATTACKS - TYPES

However gaining access to a system or network is the primary goal of an attacker, these intrusions are classified further based on how they are carried out. Hackers may also originate from inside the network (internal attackers) or from outdoor the network (external attackers) (outside attackers). For these attackers, the internet is the most common method of intrusion.

6.1. DoS - Denial of Service Attack

A DoS attack's main purpose is to overwhelm resources like computing and memory, causing genuine users' requests to be denied. It increases the demand on a server or network artificially, preventing users from accessing these resources. Floods and flow exploitations were categorized into two categories by the Department of State. The first strategy makes use of external communication requests. The network, for example, can become overcrowded by continually sending the ping command to it. One more illustration of this sort of assault is when a client sends synchronization needs to a server for the handshaking protocol but never receives a response [14]. The second assault strategy crashes the machine or network. The assailant directs an input message to the target machine that exploits weaknesses in the system and crashes it, rendering it unreachable to anybody else. DDoS (Distributed DoS) is a sort of DoS attack that disrupts numerous systems at the same time.

6.2. User to Root (U2R) Attack

The aggressor signs into the framework with his login and password, just like any other user. The attacker assumes some responsibility after getting access in order to gain origin admittance to the system and so become the administrator [10]. There are several types of user-to root attacks, the most well-known of which is the buffer overflow attack.

6.3. Scan Attack

Ports are small openings that allow data to flow via a system or network. The transfer control protocol and the user define protocol remain the dual most common protocols that use ports for communication. An attacker uses a listening service to look for open ports and sends the packet to them [15]. They can utilize the packets to figure out what services are successively on the device, as well as the operating system. Intruders can also employ a port scanning attack to find out which hosts are connected to a network and other network information including topological data, IP addresses, MAC addresses, router, and gateway filtering systems, imposed firewall rules, and so on.

6.4. Eavesdropping Attack

The assailant listens in on other people's chats without their permission. It may be used to listen to phone calls, read emails and chat messages, and access other websites. The eavesdropping attack is difficult to detect because it has no effect on the network's usual functions [16]. Because eavesdropping is so difficult to detect, it is frequently the most difficult challenge most managers face in an activity. By means of strong encryption techniques, the data can be protected from eavesdroppers.

6.5. Man-in-the-Middle Attacks

Intercepts a discussion between two persons and impersonates one of them to obtain access to sensitive information. Despite the fact that the attacker has intercepted the conversation in the middle, the two parties believe they are speaking directly to one another. A man-in-the-middle attack, which allows the attacker to hold and alter responsive informative sources in real-time transactions, is the most serious danger to online security. The assailant may be talented to exploit weaknesses in the network's security setup. Man-in-the-middle attacks include session hijacking, side-jacking, evil twin, and sniffing [17].

Oludele Awodele et al. developed a multi-layered design strategy for intelligent intrusion detection and prevention systems. The suggested technique is made up of three layers: FAL, SRL, and CL. The FAL (File Analyzer Layer) prevents unwanted access to essential files and folders. The administrator chooses critical files and directories, which are subsequently forwarded to the file analyzer for monitoring. [18].

An Agent-Based Distributed IDS was presented by Yu Lasheng and Mutimukwe Chantal (ABDIDS). The task of detecting intrusions is delegated to autonomous and cooperative agents. Three types of agents operate together to detect intrusions: monitoring registry agents, monitoring agents, and management agents [19]. Registrars of monitoring agents are in charge of registering and identifying monitoring agents. It also provides information on the present state of all monitoring agent. Monitoring agents collect and communicate facts about node security to managing agents. By using managing agents, data is processed and intrusions are identified.

The mixture astute based Intrusion Detection System given by Jaisankar and Kannan is a half and half savvy based IDS. Include determination specialists, approval specialists, and dynamic specialists are among the three classifications of specialists utilized. Using rough sets, the feature selection agent identifies required IDS features. Validation agents validate selected characteristics and pass them to the hybrid model. Decision-making agents are employed to discern between normal and aberrant behavior. The decision manager, who recognizes the invaders, makes the final decision [20]. The EC4.5, SVM, and hybrid models are three classifiers that yield a higher detection rate.

M. Laureno et al. presented a virtual machine-based host-based intrusion detection system. Because of their lower cost and portability, virtual machines are preferred over computing systems. This solution uses an IDS that is external to the virtual system to monitor visitor actions. IDS receives data from Virtual Machine Monitor. Intruders cannot gain access to the detecting system since it is secure. This strategy can also be used to keep track of remote progressions. The reaction module restricts the execution of confined cycles with the goal that genuine clients are not hindered [21]. To build the presentation of the current IDS and reaction instrument, more work should be done on the framework. One more detriment of this procedure is the incapable interface for connecting with the portion to empower, kill, or suspend an interaction.

In remote sensor organizations, Garth Crosby et al. proposed area mindful, trust-based discovery and detachment of compromised hubs. The cycle starts by setting up standing and trust, permitting every gadget in a remote sensor organization to survey whether or not different gadgets are compromised. Assuming it is penetrated, the vital remedial move is made with the assistance of negative data trade and free trust-based direction. The concentrate additionally incorporates a direct area check strategy that utilizes got signal strength information. When there are 15 or less hubs accessible, the compromised hub location rate is great [22]. The pace of compromised hub identification drops as the quantity of hubs develops.

Utilizing Support Vector Machines and progressive grouping, Khan et al. proposed a clever Intrusion Detection System. The proposed strategy focuses on the disclosure of anomalies over the discovery of abuse. One of the most reliable classifiers, the Support Vector Machine (SVM), is utilized with least preparing time. Assuming the information is tremendous, the Dynamically Growing Self-Organizing Tree (DGSOT) calculation is used for bunching since it outflanks conventional grouping calculations [23]. The methodology is profoundly precise, with low rates of bogus up-sides and negatives.

Intrusion Detection System Using K-Nearest Neighbor Classifier was presented by Yihua Liao and V. Rao Vemuri. In this procedure, framework calls are assessed to distinguish interruption. For each program, a different information base for brief framework calls is made. A framework call's recurrence of event is utilized to depict a program's conduct. All system calls are stored in a database as tuples. K-nearest neighbor looks for patterns that are the most similar to an unknown tuple. The tuples are categorized here based on the majority votes of their neighbors [24]. Intrusions are identified using a mix of statistical approaches. Large computations and storage are required to complete tasks. The algorithm can be made more efficient by using parallel hardware.

Dewan M. Farid et al. introduced an exploration on versatile interruption discovery utilizing a choice tree and a Nave Bayesian Classifier. Conventional learning calculations in IDS have a high bogus positive rate, which is an issue. The utilization of a Nave Bayesian Classifier related to choice tree-based learning further develops balance discovery and lessens bogus positive rates. In the preparation set, this procedure additionally distinguishes different types of assaults and eliminates copy credits [25]. The methodology has a high location rate and a significant degree of precision. The KDD99 dataset was utilized to assess this methodology, and it recognized interruptions with almost 99% precision and hardly any bogus up-sides.

R. Shanmugavadivu and N. Nagarajan presented a work on a fuzzy logic-based IDS. Most IDS rely on a thorough understanding of numerous threats to ensure that the system can handle any situation. This reliance is reduced in this article by employing fuzzy logic, which efficiently detects anomalous network activity [26]. Because the rule base has a collection of better and updated rules, accuracy is obtained. The rule foundation is built by sifting through attacks and normal data for single-length common items. From that point onward, indistinct guidelines are picked and taken care of into the fluffy framework for information characterization testing.

Emma Ireland et al. presented a work that used a GA (Genetic Algorithm) and FL (Fuzzy Logic) to detect intrusions. First, the approach creates procedures at random, and the quality of the rules is increased throughout the training phase by utilizing a fuzzy genetic algorithm. Each feature of a record corresponds to a set of rules. The trapezoidal fuzzy rule is used to compute the attack's degree of certainty using parameters from each block. To classify an occurrence as an attack or regular behavior, the total of certainty of each block is compared to an administrator-defined threshold value [27]. Unlike typical genetic algorithms, this fuzzy genetic algorithm identifies unidentified assaults. This technique is quite good at identifying denial of service attacks.

Many reviews of security algorithms in many domains have been published in the literature by various researchers. [28][29][30][31]]. This research will undoubtedly provide researchers with the concept of using intrusion detection techniques in many applications. [32][33][34]. Intrusion detection strategies were also discussed in many problems [35].

7. CONCLUSION

Personal Computer network security is a mind boggling subject that includes numerous parts of PC innovation, network the board, network utilization, and organization upkeep. For wellbeing concerns, we should blend various programming to build PC network security. It is basic to growing more compelling security-settling measures to further develop PC network security. It will consume most of the day to guarantee the ordinary activity of enormous scope network frameworks and interchanges, just as to keep an economical and efficient transportation organization. Without a question, infiltration has become a perilous reality for numerous firms in terms of safeguarding their critical information and resources. This study thoroughly examines intrusion detection schemes. All of the procedures are used to try to find intrusion in any way possible. Hackers, on the other hand, are able to come up with new methods and concepts to get around security standards. Network Intrusion Detection System with Fuzzy Logic22, for example, detects intrusion with high accuracy using a rule foundation. However, creating a fuzzy model and fine-tuning it is a challenging task. So far, only a few approaches have a greater false alarm rate. As a result, any intrusion detection system must have a high degree of precision, a low rate of false positives and negatives, as well as low computational, duration, and cost overheads.

8. Acknowledgement

The authors are grateful for the facilities provided by CHRIST (Deemed to be University), Bengaluru and Bharath Institute of Higher Education and Research (Deemed to be University), Chennai for the facilities offered to carry out this work.

References

1. Translated by Cheng Peiqing, et al. Computer network security. Publishing House of Electronics Industry, (1994).9
2. Li Wenlong. Face to face with a hacker. Internet world.1999 (2):2~8
3. Xiao Ze. Research on computer network security analysis model [J]. Journal on Communications, 2012:269.
4. Z.hang Cheng. Research on computer network security analysis model [J]. Practical Electronics, 20l3(v):148-149.

5. Hong Yaling. Research on computer network security analysis model [J]. Computer CD Software and Applications, 2013(z):1-152.
6. Wang Yuan. Quantitative Evaluation Method of Network Security Situation [D]. Ph.D. Dissertation, university of science and technology, 2003.
7. Cui Jing, Liu Guangzhong, the basics of computer network [J]. Tsinghua University Press, 2010.
8. Wang Wenbing, security of computer network [J], Tsinghua University Press, 2010.
9. Akyildiz IF, Xie J, Mohanty S. A survey of mobility management in next-generation all-IP-based wireless systems. IEEE Wireless Communications. 2004 Aug; 11(4):16–28.
10. Srinivasan T, Vijaykumar V, Chandrasekar R. A self-organized agent-based architecture for power-aware intrusion detection in wireless ad-hoc networks. International Conference on Computing and Informatics. ICOCI'06. IEEE; 2006. p. 1–6.
11. Garcia-Teodoro P, Diaz-Verdejo J, Marcia-Fernandez G, Vazquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers and Security.09; 28(1 2):18–28.
12. Wang K, Salvatore J, Stolfo SJ. Anomalous payload-based Network Intrusion Detection. Recent Advances in Intrusion Detection. Springer: Berlin Heidelberg; 2007. p. 203–22
13. Bose A, Hu X, Shin KG. Behavioral detection of malware on mobile handsets. Proceedings of the 6th International Conference on Mobile Systems, Applications and Services. ACM; 2008. p. 225–38
14. Qu Y, Lu Q. Effectively mining network traffic intelligence to detect malicious stealthy port scanning to cloud servers. Journal of Internet Technology. 2014 Sep; 15(5):841–52.
15. Sisalem D, Kuthan J, Ehlert S. Denial of service attacks targeting a SIP VoIP infrastructure: Attack scenarios and prevention mechanisms. IEEE Network. 2006 Sep-Oct; 20(5):26–31.
16. Luo M, Peng T, Leckie C. CPU-based DoS attacks against SIP servers. IEEE Network Operations and Management Symposium, NOMS 2008; Salvador, Bahia. 2008 Apr 7-11. p. 41–8.
17. Kim J, Lee JH. A slow port scan attack detection mechanism based on fuzzy logic and a stepwise policy. 4th International Conference on I ntelligence Environments; Seattle, WA. 2008 Jul 21-22. p. 1–5.
18. Zhang Z, Li Y, Man ZX. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping- induced channel loss. Physics Letters A. 2005 Jun; 341(5-6):385–9.
19. DesmedtY. Man-in-the-middle attack. Encyclopedia of Cryptography and Security. Springer: US.11. p. 759–9.
20. Awodele O, Idowu S. A multi-layered approach to the design of Intelligent Intrusion Detection and Prevention System (IIDPS). Issues in Informing Science and Information Technology. 2009 Jan; 6(1):631–47.
21. Lasheng Y, Chantal M. Agent Based Distributed Intrusion Detection System (ABDIDS). Second Symposium International Computer Science and Computational Technology (ISCSCT'09); 2009 Dec 26-28. p. 134–8.
22. Laureano M, Maziero C, Jamhour E. Protecting host-based intrusion detectors through virtual machines. Computer Networks. 2007 Apr; 51(5):1275–83.
23. Crosby GV, Hester L, Pissinou N. Location-aware, trust based detection and isolation of compromised nodes in wireless sensor networks. IJNS 2011; 12(2):107–17.

24. Khan L, Awad M, Thuraisingham B. A new Intrusion Detection System using Support Vector Machines and hierarchical clustering. The VLDB Journal 2007, Oct; 16(4):507–21.
25. Liao Y, Rao Vemuri V. Use of k-nearest neighbor classifier for intrusion detection. Computers and Security. 2002, Oct; 21(5):439–48.
26. Farid DM, Harbi N, Rahman MZ. Combining Naive Bayes and decision tree for adaptive intrusion detection. International Journal of Network Security and its Applications. 2010; 2(2):12–2.
27. Ireland E. Intrusion detection with genetic algorithms and fuzzy logic. UMMC Sci Senior Seminar Conference; Morris, MN. 2013, p. 1–30.
28. RM Gomathi, JML Manickam, A Sivasangari, P Ajitha,"Energy efficient dynamic clustering routing protocol in underwater wireless sensor networks", International Journal of Networking and Virtual Organisations, Vol.22,4 pp. 415-432
29. Kanyadara Saakshara, Kandula Pranathi, R.M. Gomathi, A. Sivasangari, P. Ajitha, T. Anandhi, "Speaker Recognition System using Gaussian Mixture Model", 2020 ,International Conference on Communication and Signal Processing (ICCSP), pp.1041-1044, July 28 - 30, 2020.
30. Sivasangari, A., Ajitha, P., Brumancia, E., Sujihelen, L., Rajesh, G.(2021),” Data security and privacy functions in fog computing for healthcare 4.0”,Signals and Communication Technology, 2021, pp. 337–354
31. A Sivasangari, P Ajitha, RM Gomathi, "Light weight security scheme in wireless body area sensor network using logistic chaotic scheme", International Journal of Networking and Virtual Organisations, 22(4), PP.433-444, 2020
32. Sivasangari, A., Nivetha, S., Pavithra,, Ajitha, P., Gomathi, R.M. (2020),” Indian Traffic Sign Board Recognition and Driver Alert System Using CNN”, 4th International Conference on Computer, Communication and Signal Processing, ICCCSP 2020, 2020, 9315260
33. Gowri, S. and Divya, G., 2015, February. Automation of garden tools monitored using mobile application. In International Confernce on Innovation Information in Computing Technologies (pp. 1-6). IEEE.
34. Gowri, S., and J. Jabez. "Novel Methodology of Data Management in Ad Hoc Network Formulated Using Nanosensors for Detection of Industrial Pollutants." In International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 206-216. Springer, Singapore, 2017.
35. Sivasangari A, Bhowal S, Subhashini R "Secure encryption in wireless body sensor networks",Advances in Intelligent Systems and Computing, 2019, 814, pp. 679–686
36. Subhashini R, Niveditha P R, "Analyzing and detecting employee's emotion for amelioration of organizations", Procedia Computer Science, 2015, 48(C), pp. 530–536
37. Ajitha, P.Sivasangari, A.Gomathi, R.M.Indira, K."Prediction of customer plan using churn analysis for telecom industry",Recent Advances in Computer Science and Communications,Volume 13, Issue 5, 2020, Pages 926-929.