Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 3101-3109

Research Article

Real Time Network Security Intrusions and Risk Management: A Survey

Bashayer O. ALOFFI[1], Mohammed A. AlZain[1], Mehedi Masud[1,*], NZ Jhanjhi[2], Jehad Al-Amri[1], Mohammed Baz[1]

[1]College of Computers and Information Technology, Taif University,
P.O. Box 11099, Al-Hawiya-Taif, 21944, Saudi Arabia
[2]School of Computer Science and Engineering, SCE, Taylor's University, 47500, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract

Due to the massive use of the Internet by people, institutions and organizations for many reasons, so they need to make sure that all their information is safe and free from tampering with their information, theft, disclosure, and misuse of it in a way that could harm them. In general, no one can be able to find an Internet, organizations, companies, or even users' personal devices that are not threatened by security breaches, intrusions, and any kind of attacks. This paper surveys recent researches related to network security intrusions and risk management. In addition, this work aims to clarify how to detect illegal intrusions. Furthermore, evaluate and control risks and reduce them to acceptable levels. Also discussing strategies for managing them.

Keywords: Network security, risk management, data integrity, intrusion.

1. Introduction

Nowadays, the use of the internet has significantly increased all over the world so secure the network from intrusive actions and attackers became essential issues recently for sure[3]. Meanwhile, detecting and preventing intrusions using new methodologies and working to develop and update them constantly is an important requirement and the reason for this is the development of attacks and intrusions and the emergence of new types that require us to constantly be attentive to protect our data and information. And this made detection and prevention one of the most important issues in the field of network security. And the occurrence of these intrusions greatly made them cause huge losses that harm organizations and companies, and even at the personal user's devices, so they badly need to protect their data.

This paper focuses on the issues related to network intrusions and risk management. Today an enormous number of procedures are performed via the internet and thus drive to have a danger of data larceny and abuse. Detect of the Intrusion strategies are hence evolved and enforceable to the organizations and users' PCs to identify such meddling activities and caution the administrators. It is important to clarify how the rest of the paper will be arranged as follows. Section 2 describes the intrusions and the IDS and IPS and its types. In addition, Section 3 illustrate types of attacks. Section 4 discusses Denial of Services DOS. Section 5 will clarification data integrity. Section 6 will present risk management. Section 7 presents suggestions for future work and finally conclude the paper.

2. Background

The security of the network is a domain where any user or company must protect their networks from any malicious threats external or internal attacks[6]. The intrusion detection systems (IDS) can sense external threats from intruders. Meanwhile, before they occur intrusion prevention systems (IPS) can avoid them. These strategies, in exchange, allow us to shield our processes and our data from exposure.

2.1 Intrusion Detection System IDS

The National Institute of Standards and Technology (NIST) classifies intrusion detection as [8] "the process of monitoring the events occurring in a computer system or network and analysing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network". It is very important to protect the network and the system from the intruders[11]. Intrusion is known as when the attackers attack the network or the computer system and causes a real damage in the information or even in the hardware of the computers or servers through unauthorized access or sometimes by authorized access to gain some privilege.

The combination of hardware or software modules that give observation of computer systems and announces the administration if an attack occurs is denominated as IDS which is stand for intrusion detection system. IDS utilize two approaches to detect any intrusion with the signature-based IDS and anomaly-based IDS. According to Kumar, Vinod al [2], To assist in analysing the network, a secure anomaly-based IDS controlled by a machine is might be a more realistic technique. The determination of the stream of the network and concentrate on the detection and recognition of uncommon network activity and arrange them into assaults called (ADS).

At SRI International, Dorothy Denning has been introduced the first design to detect the intrusion. several IDSs

to detect any intrusions have been suggested in the academic and business world [4]. A. Borkar, A. Donode, and A. Kumari illustrates in spite of the fact that thus systems are incredibly assorted in the methods they utilize to accumulate and processing data, the greater part of them depend on a moderately broad compositional structure which comprises of the accompanying segments:

- **Data collection module (sensor)**

  From the tracked device It is mainly accountable for gathering data.

- **Detector (Detection ID review engine for intrusion)**

  To detect intrusive behaviors, the data that obtained from sensors processed.

- **Information obtained by sensors exists in the knowledge stem (database) includes but in pre-treat format**
  (e.g. data profiles, attack and signature knowledge base, filtered data, etc.).

  Such information is normally collected by security and network specialists.

- **Configuration tool.**

  Provides updates on the current status of the IDS intrusion detection device.

- **The response portion initiates make actions upon sensing an intrusion**

  Such responses may either be automatic (active) or require (inactive) human activity as figure 1 shows the whole construction of the IDS [4].

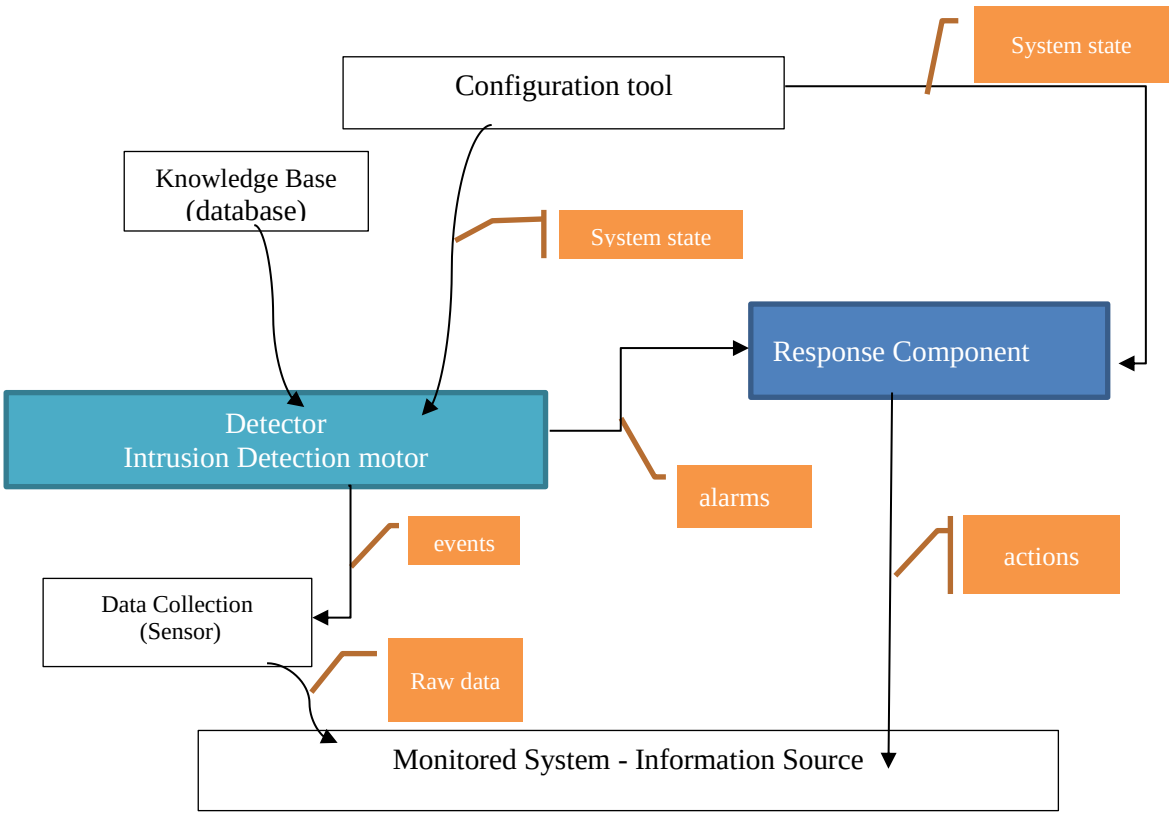

Fig. 1. Intrusion detection system (IDS) basic construction.

2.1.1 Classification of Intrusion Detection System

This section will present the software to detect the Intrusion which classified into three major types. Overall,

system of detect host intrusion looking at host computer behaviour and files. Whereas, network traffic observed by system of detect network intrusion and system of detect network node intrusion.

2.1.1.1 Network Intrusion Detection System NIDS

The bulk of corporate intrusion detection devices are network-based. Capturing and processing network packets, these IDSs track attacks [8]. Approximately spread out or implanted at Strategic points across the network to protect all areas when traffic is more likely destined to be defenceless against attacks. In general, it is typically extended to the whole subnets and aims to matching any traffic that passes through a random attack's library. It analyses network traffic passively across the network that the points located on which it is deployed. It can be comparatively easy to protect and not easy for the intruders detecting it. So that means if any intruders attack the network, they could not realize that NIDS is detection their attacks. Meanwhile, a large measure of the network traffic is examined, which involve also have minimal particularity. This means they may usually miss an attack occasionally or may not notice anything was happen in traffic that was encrypted. There are many advantages and disadvantages of Network-Based IDSs such that [8]:

1. Few well-placed IDS-based networks can track a wide network.
2. There is no effect on the current network while implementation of network intrusion detection systems. Usually, there are quiet instruments that listening to the wire of the network and never interaction within the regular activity of a network which is network based IDSs. As a result, it is typically easy to update the network to provide network intrusion detection systems within minimum striving.
3. It is possible to make network based IDSs very safe against attacks and also make them hidden to certain attackers.

While the disadvantages are [8]:

1. Network-based IDSs can have trouble handling all packets on a wide or occupied network, so an attack conducted during times of heavy traffic may not be recognized. Some developers are seeking to address this issue by fully integrating the IDS in hardware (HW), which is plenty easier and faster. The requirement to rapidly evaluate packets also forces developers to detect less attacks as well as to detecting attack with as few computational powers as potential that may limit detection performance.
2. Widely of the benefits of network intrusion detection system do not extend too much modernistic switch-based networks. Switches break networks into several tiny segments (using Ethernet wire which is fast pursuant to the host) which have dedicated communications between hosts served by the aforementioned switch. Restricting the network intrusion detection system sensor surveillance distance to a one host because much of switches don't having uniform tracking ports. Also where those control ports are supported by switches, all traffic passing through the switch sometimes cannot reflect by a single port.
3. Protected information will not be analyzed by network based IDSs. If more companies and malicious users use VPN services, so this issue will increase.
4. Many network intrusion detection systems are unable to say either an assault is actually occurring or not and if It has been effective, but they only can know that an assault has been launched. This implies after an attack is identified by a network intrusion detection system each host was attacked must be manually investigated by administrators to determine if it has also been infiltrated.
5. From the disadvantages also that network intrusion detection systems have issues dealing with network Attacks that include packets being fragmented. The misshapen packets cause intrusion detection systems to crash and become dysfunctional [8].

And many other disadvantages.

2.1.1.2 Network Node Intrusion Detection System NNIDS

From a network to a host conducting a traffic review is known as Network Node-based IDS. NNIDS and NIDS not the same and the differentiation between them is that traffic is tracked only on a single host, not on a subnet as a whole [15].

2.1.1.3 Host Intrusion Detection System HIDS

Because of their capabilities to take a closer look at the traffic of the internet ,HIDS has several benefits over NIDS, and as a secondary line of protection toward malicious packets that a NIDS has struggled to detect it. It checks at the whole file collection of the device and upon the file package it matches it to the existing "snapshots". It then investigates whether outside regular business usage there are major variations and warns the superintendent as to for certain if any were enough incomplete or substantially changed documents or settings. It mostly uses host-based behaviour such as program use and documents and directories, system-wide file access,

and logs of kernel. Attacks that a network intrusion detection system does not see can be observed by the HIDS. Furthermore, in an area when the traffic of the network is encoded in it, it can work. The most popular ways of communicating this description are the two types of intrusion detection systems which are network and host, and in this area, you won't see NNIDS listed very much. Just assume it is more of a NIDS kind [19].

2.1.2 Approaches of Intrusion Detection System

This section will present the two mean approaches uses in the intrusion detection system known as the anomaly detection system and signature detection system.

2.1.2.1 Anomaly Detection System ADS

With the rapid growth and wider implementations in fields such as enforcement, surveillance, financial supervision, AI security, and risk management which this paper is interested in, so a significant role played by anomaly detection for detect the intrusions and protect the network is becoming important and it illustrated in cultural diversity. Outlier detection which the anomaly detection is known as it's is outlined as the method of identifying data sample that deflects substantially from other data precedent cases [1]. As [7],[14],[1],[2] illustrate, anomaly intrusion detection definition in networks Relevance is made to the issue of identifying extraordinary trends in the traffic of the network that is not in line with the planned normal Behavior. These non-conforming trends are also called deviations, aberrations, outliers, and variations. Detection of anomaly has wide implementations in those areas as fraud prevention for bank cards, cyber intrusion detection Protection and army monitoring of enemy movements. For more Explanation, an anomalous pattern of traffic on any network can conclude that a compromised device sends out a sensitive information to an illegitimate user [7].

2.1.2.2 Signature Detection System SDS

A signature-based intrusion detection system process and device are revealed. The definition of it is the procedure of network intrusion detection usually consists of keeping signature profile information that recognizes patterns related to network interferences in a database of signature and creating a prediction model based on patterns of the signature. The packets of the data generated by connected over the computer network and getting a matched prediction model are categorized according to the classification rules created. Classified the packets of the data are placed to the engine of signature for corresponding with the profiles of signature [16]. An important concept related to the signature detection system is called SNORT. Is a commonly used network built on an open-source signature intrusion detection system, which utilized for the logging and visualization of actual traffic over Network connections? SNORT currently has a robust archive of over 1,000 assault signatures. 3 major forms wherein the SNORT could be programmed, including packet logger, sniffer, and the intrusion detection system network. SNORT watches and constantly shows network packets on the device In sniffer mode [9],[19].

- Alert (using the chosen alert process, raise the alarm and then record the Package).
- Activate (produce an alert then move to another complex rule).
- Log (Logging the evaluated packet).
- Dynamic (produce an alert and then move to another complex based).
- Pass (skip the packet analyzed) [19].

2.2 Intrusion Prevention System IPS

Detecting network or device operations for malicious actions using network monitoring software**.** IPS used first before using IDS and when the intrusion prevention system failed to deter the attacks or threats then IDS should detect it before any damage occurs to the computer systems. IPS is a technique that analyse the traffic of the network stream to expose vulnerability exploits and prevention it to ensure the security of the network by using preventative mechanisms. The firewall behind it immediately The IPS also sits and offers a supplementary research layer. Continuously works by examining and analysing transmitted network traffic for malicious purposes and established known vulnerabilities and taking four automated actions which is [13]:

- Raise and sending an alarm to the administrator.
- Throwing out suspicious packages.
- Traffic blocking from the origin address.
- Resetting the connection again.

2.2.1 Classification of Intrusion Prevention System IPS

There are four mean types as summarized in the figure:

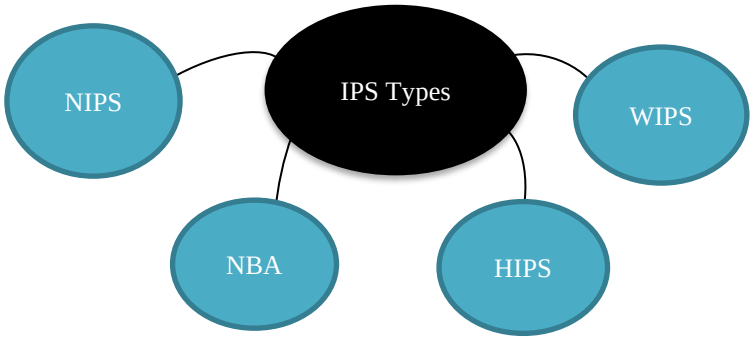

Fig. 1. Types of Intrusion Prevention System.

2.2.1.1 NIPS Network intrusion prevention system
Through monitoring protocol behaviour, it tracks the whole network for suspect traffic.

2.2.1.2 WIPS Wireless intrusion prevention system
Through observing wireless network protocols, it tracks wireless networking for suspect traffic.

2.2.1.3 NBA Network behaviour analysis
To detect risks creating irregular traffic patterns, it analyses network traffic.

2.2.1.4 Host-based intrusion prevention system HIPS
It is known as automated software program that through examining events occurring within this host, operates a one host for extremely unlikely operation.

3. Types of Attacks

All the attacks classify into two types which are either passive attacks or active attacks. The aim of the active attack is to destroy the computer systems or network and caused real damage[20].[21].

Meanwhile, the passive attacks just want to earn information by monitoring the transmissions of the data over the network and dose not modify the data or harm computer system at all. The types of active attacks are Masquerade (spoofing), reply attacks, denial of service, man in the middle attack, modification on data, Trojan, viruses' theses all are example of active attack which can harm the computer system and threat the security. The passive attack attempts gain knowledge or making use of system knowledge, but it does not impact system capacity [2],[5],[4].

Eavesdropping, traffic analysis, scanning is example of passive attack. The attacker can classify into three mean categories which is based on the attacker's locations, based on the attacker's aim, based on the attacker's skill. The one that based on the attacker's location is divided into insider and outsider attacker. The insider attacker could have authorized access to that organization or company and do it to get more privilege or many reasons by the destructive attack on a computer or network device is carried out. But the outsider attack is attempted to destroy and manipulated with that information or get advantage of it [22].

3.1 Eavesdropping Attack

Eavesdropping is a type of passive attack and it all about unsecured network communications which allows an attacker to read data. The best attack application of eavesdropping is that an attack called a man in the middle as figure 3 shows that the eavesdropper can read the data that transferring via the communication between Alice and Bob without they know [4].

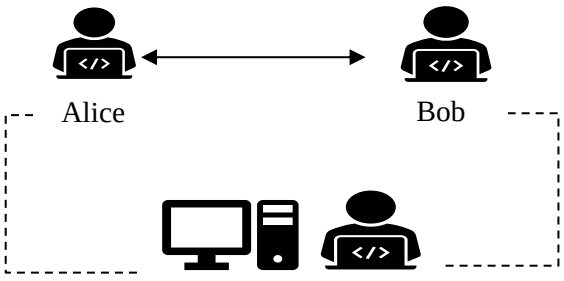

Fig.3. Attack of Eavesdropping

3.2 Masquerade (spoofing)

As Schuckers, Stephanie AC mentioned [17] , it is a case in which an entity pretends to be one of the legitimate entities to obtain the benefits of this entity such as passwords, credit card, etc.

3.3 Modification of Data

Simply It means that some portion of a message is altered or that message is delayed or reordered or delete part of it just to produce an unwanted and unauthorized effect.

3.4 Brute force attack

An active attack an experimentation strategy used to acquire data, for example, passwords, or (Personal Identification Number) PIN. A word reference assault looks through assaults rule-based hunt assaults and it is brute force type of attacks. As shown in figure 4 the adversary or the attacker tries multiple random passwords until one of them come true and this attack can avoided by having a strong password [4],[5].

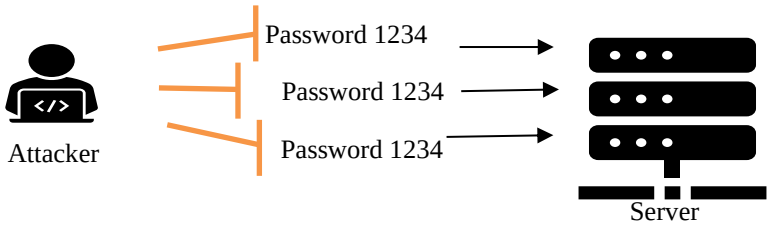

Fig.4. Brute force attack.

3.5 Traffic analysis

Analysis the traffic is defined as the method of intercept and process communications in attempts to interpret data from traffic flows that can be carried out even though the messages that encoded.Generally, The more packets that are detected, or even captured, the more traffic can be observed [5].

3.6 Replay

During the transmission a valid data is maliciously or counterfeit repeated or delayed. This is carried out either by the originator or by an adversary and it is occurring after a hacker captured and altered a key part of a message [12].

3.7 Black hole attack

According to Mohan V. Pawar1 and Anuradha J2 [5] **,** One of several advancements targeting that opponent using the protocol called routing to announce themselves as providing the fastest route to the nodes which packets it needs to intercept is the Black Hole attack. An attacker using the flooding-based protocol to list the initiator's demand for a direction, then produces a return message from the hacker that to the recipient that has the short route. When the message comes from the adversary hit the initiator just before respond from the original node, so it is considered the shortest route to the recipient that the initiator would consider. But it produces a suspicious virtual path.

3.8 Wormhole

The tunnelling intrusion is often what this attack called. An attacker obtains a packet at that stage in this attempt and pipes it to some other compromised network interface [5]. So a beginner believes that the shortest route was discovered at the network. [10].

4. Denial of services DOS

As [5] and [2] illustrate the concept of availability of security priorities threatened by DOS attack. It is basically designed to prevent normal use of communication facilities by shut down or make the system inoperable. It is occurred when a program or node uses all its resources it could crash the entire system.

- Distributed Denial of Services DDOS

Denial of Service Attack (DDoS) an intrusion in which several networks have been infiltrated by a malicious software (Trojan horse). They are vindictively used to attack a unified system. The assault tends to lead to the rejection with a certain operation to the target device. In the DDoS attack, all of the devices used to launch an attack and the target system both considered casualties of the assaulted.

5. Data Integrity

Data integrity it is the greatest important things about data security[23],[22],[24]. And it is the ensure of that no one modify or manipulated with the data during the transmission over the network[25].

6. Risk Management

Risk management approach to computer security. A proper risk methodology could be a helpful tool for solving the risk management problem. In a certain system, risks are evaluated by determining expectations, calculating the effects of adverse events, forecasting the probability of such occurrences, and evaluating the benefits of alternative courses of acts. [18]. The concept of Risk management basically is a regulatory mechanism in which potential risk assessment techniques are considered and decisions on appropriate risks are taken. Furthermore, could use this to compute the risks comes from intrusion and achieve good security systems comprise of strategic alternatives that effectively affect hazard, including the decrease, expulsion, or redistribution of danger. Eventually, an adequate degree of danger is resolved and a technique for accomplishing that degree of danger is embraced.

Table 1 present the real-time intrusions and risk management in previous research over the period between 2020 to 2005. And the related research's with intrusion detection and prevention systems in past few years. Furthermore, discusses the mechanism and approaches that applied on IDS and IPS that can make the system an environment[11] more secure for the organizations, companies and user's devices.

				Type of Attack		Approaches of IDS		
Ref	Year	Detection Intrusion System	Prevention Intrusion System	Passive Attack	Active Attack	Anomaly IDS	Signature IDS	Risk Management
[1]	2020	✓				✓		
[2]	2020	✓		✓	✓	✓		
[4]	2017	✓	✓	✓	✓			
[5]	2015		✓	✓	✓			
[7]	2013	✓				✓		
[9]	2012	✓					✓	
[10]	2011	✓	✓					
[12]	2010			✓	✓			
[13]	2009		✓					
[14]	2009					✓		
[15]	2009	✓						
[16]	2008	✓					✓	
[17]	2002				✓			
[8]	2001	✓	✓			✓	✓	
[18]	2000							✓
[19]	2005	✓						

Table 1 present the real-time intrusions and risk management in previous research

7. Conclusion & Future work

While attacks are constantly evolving, we need to innovate and develop new defenses technologies against network hackers, adversary and attackers. At the end of this paper we need to make sure that the ability to identify and

manage risks developed. Furthermore, the techniques of detection and prevention the intruders are being developed to ensure safety. All this in order to make the Internet environment a safe environment to use.

For future work, since every day there is a new attack, we aim to develop a modern IDS and IPS techniques case the attacker always having a new way to attack because the attackers on the network do not give up and every time they try to attack the defences of the systems and destroy it with new attacks and unauthorized intrusions on the systems and manipulated with users and organizations data. Therefore, we need to develop our defence's techniques to repel their attacks and protect the systems and security of our computers, and servers.

References:

1. Pang, G., et al., Deep learning for anomaly detection: A review. arXiv preprint arXiv:2007.02500, 2020.
2. Kumar, V., et al. Detecting Intrusions and Attacks in the Network Traffic using Anomaly based Techniques. in 2020 5th International Conference on Communication and Electronics Systems (ICCES). 2020: IEEE.
3. Samra, H., et al., Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems. Health Information Management Journal, 2019. **49**(2-3): p. 117-126.
4. Borkar, A., A. Donode, and A. Kumari. A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). in 2017 International Conference on Inventive Computing and Informatics (ICICI). 2017.
5. Pawar, M.V. and J. Anuradha, Network security and types of attacks in network. Procedia Computer Science, 2015. **48**: p. 503-506.
6. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
7. Bhuyan, M.H., D.K. Bhattacharyya, and J.K. Kalita, Network anomaly detection: methods, systems and tools. Ieee communications surveys & tutorials, 2013. **16**(1): p. 303-336.
8. Bace, R. and P. Mell, NIST special publication on intrusion detection systems. 2001, BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.
9. Kumar, V. and O.P. Sangwan, Signature based intrusion detection system using SNORT. International Journal of Computer Applications & Information Technology, 2012. **1**(3): p. 35-41.
10. Sharma, K., N. Khandelwal, and M. Prabhakar. An overview of security problems in MANET. in ISEM International Conference. 2011.
11. Sodhi, G.K., et al., Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code. Indonesian Journal of Electrical Engineering and Computer Science, 2018. **12**(3): p. 1297-1304.
12. Rai, A.K., R.R. Tewari, and S.K. Upadhyay, Different types of attacks on integrated manet-internet communication. International Journal of Computer Science and Security, 2010. **4**(3): p. 265-274.
13. Sun, Y. and F. Khan, Score-based intrusion prevention system. 2009, Google Patents.
14. Chandola, V., A. Banerjee, and V. Kumar, Anomaly detection: A survey. ACM computing surveys (CSUR), 2009. **41**(3): p. 1-58.
15. Fawzy, S.S. and A.M. Yousif, NETWORK NODE INTRUSION DETECTION SYSTEM. Iraqi Journal of Science, 2009. **50**(3): p. 396-402.
16. Elijah, A. V., Abdullah, A., Jhanjhi, N., Supramaniam, M., & Abdullateef, B. (2019). 'Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: An empirical study. Int. J. Adv. Comput. Sci. Appl., 10, 520-528.
17. Schuckers, S.A., Spoofing and anti-spoofing measures. Information Security technical report, 2002. **7**(4): p. 56-62.
18. V. Singhal et al., "Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned Railway Level Crossings," in IEEE Access, vol. 8, pp. 113790-113806, 2020, doi: 10.1109/ACCESS.2020.3002416.
19. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology, 12(1), 8-15.
20. Alshambri, H., et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 2020. **8**(1).
21. Alhathally, L., et al., Cyber security Attacks: Exploiting weaknesses. International Journal of Recent Technology and Engineering 2020. **8**(5).
22. Altwairqi, A.F., et al., Four Most Famous Cyber Attacks for Financial Gains. International Journal of Engineering and Advanced Technology, 2019. **9**(2).
23. AlZain, M.A. and J.F. Al-Amri, Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform. International Journal of Applied Engineering Research, 2018. **13**(8): p. 6380-6387.
24. Faragallah, O.S., et al., Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications. IEEE Access, 2020.

25. AlZain, M.A., et al., Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 207-221.