Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature

Sangeetha Prabhu[1] & Subramanya Bhat[2]
[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India
[2]College of Computer Science and Information Science, Srinivas University, Mangalore, India
E-mail: sangeethaprabhu96@gmail.com

Area of the Paper: Information Technology.
Type of the Paper: Review Paper.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3978912.
Google Scholar Citation: IJCSBE.

How to Cite this Paper:
Prabhu, Sangeetha, & Bhat, Subramanya (2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 4*(2), 40-64.
DOI: http://doi.org/10.5281/zenodo.3978912.

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature

Sangeetha Prabhu[1] & Subramanya Bhat[2]
[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India
[2]College of Computer Science and Information Science, Srinivas University, Mangalore, India
E-mail: sangeethaprabhu96@gmail.com

ABSTRACT

Cyber-attacks are becoming more common and over the last decade, many attacks have made top news, targeting manufacturing firms and governmental organisations. Such attacks have triggered substantial financial damage and they've been trying to obstruct key public sector operations. Furthermore, as the Internet of Things (IoT) has arisen, the number of Internet-connected devices is increasingly growing and being an easy target of cyber-attacks. To counter cyber-attacks, information security researchers rely extensively on intrusion detection systems (IDSs) that can identify suspicious activities by comparing patterns of documented attacks or detecting anomaly-based activities. This survey aims to tackle Trust, Protection, identification and activity on wide scale networks and Internet of Things. The proposed research aims at developing a practically deployable cyber security solution to one or more of the cyber-attacks. Multi-Stage Attacks (MSAs), APT, DoS attacks, wireless injection attacks, botnets or other malicious activities will be investigated. In this literature survey, we are highlighting the work Performed throughout the area of cyber security by various researchers, various types of cyber-attacks and its stages, various approaches to prevent cyber-attacks, different challenges faced by a preventer, and some gaps in the research. This literature review is carried out by using the secondary data obtained from peer-reviewed journals and other sources on the web. This review aims to explain Detecting Malicious Activities in Network Traffic.

Keywords: Cyber Security, Mitigation, Internet of Things, Machine Learning, Malicious Activities.

1. INTRODUCTON :

We're never going to envisage the world without the Internet at present. In every commercial enterprise, research institutes, academic institutions, economy, defence, businesses, etc., all are purposely or inadvertently focused on the Internet. In government bodies, services are delivered via the internet to any individual person in the country, as rural areas cannot operate offices for all government plans. Via these services, people are thus related to the Internet. Digital retail has become one of the decade's largest growing sectors, with customers ordering items online and selling and purchasing products from regular foodstuffs to heavy and costly appliances on the Internet (Verma et al., 2015) [1]. Online retail has now seen a huge rise in online money transfer, with internet banking, cash deposits and additional bills being paid to them. The Web continues to endure this period on a regular basis and keeping it seamless and safe is among the most appropriate methods for educational organizations.
Cyber Security can be an option characterized as the protection of virtual space systems, data and networks. This applies to the techniques used for preventing information from being stolen, compromised or targeted. Because of heavy dependency on computers in a capitalist world industry that stores and transmits an abundance of people's sensitive and vital information, cyber protection is a critical feature and many companies need insurance. We live in a digital age that recognizes how insecure our personal data is than ever before. We all live in a networked environment, from internet

banking to government infrastructure, where information is stored on computers and other devices (Buczak, Anna L. Guven, 2016) [2]. A part of the data may be sensitive information, whether it involves intellectual property, personal information, financial data or other types of data for which unauthorized entry or disclosure can have negative consequences. Cyber-attack is now an international problem and has raised many fears that hacks and other security assaults could place the global economy in danger. The organization transmits sensitive data across networks and to other devices throughout the course of business operations, and cyber security determines the information and the methods used to process or store it to secure it. Since a case of cyber strikes increases, businesses and organizations need to take measures to protect their confidential business and personal information, particularly those that deal with information related to national security, financial records or health.

Cyber security is a complex problem that involves multi-dimensional, multi-layered interventions and responses across several domains (Hoque, Sazzadul Mukit, 2012) [3]. This has proven a problem for governments as it includes numerous departments and ministries. It is more complicated because of the stable and the positive varied nature of the risks and the failure to devise an appropriate solution in the lack of particular measure perpetrators. Thanks to the rapid growth of information technology (IT) and related commercial applications, Cyberspace has grown significantly in its short lifetime. Advances in information and communications technology have revolutionized government-developed science, educational, and commercial infrastructures (Roopak et al., 2019) [4]. IT services is an important part of core services supporting national resources such as electricity, telecommunications, defence systems, emergency communication systems, power grids, space, financial systems, land records, transportation, law enforcement, security and air traffic control networks, basic public services and utilities, to name just a few. Both of these infrastructures are increasingly dependent on data relays for communication and business transactions. The operational stability and safety of critical information infrastructure is vital to the country's economic security (B, 2014) [5]. More problems are raised by the changing design of the telecommunications network. The extension of wireless connectivity to individual computers and networks is making it increasingly difficult to establish physical and logical network boundaries. The risks are introduced by growing interconnectivity and accessibility to computer-based systems which are central to the economy of the country.

Interconnectedness has become key to branches of government, education, essential infrastructure and culture. Various sensitive regional, public, private, and military infrastructural facilities may be susceptible to attacks as they still rely on outdated traditional approaches to security rather than sophisticated, robust, cyber defence (Seissa et al., 2017) [6]. Cybercrimes, cyber attacks and cyber terrorism are indeed concerns that govern data security. Cyber terrorism and traditional terrorism share several main features, and a similar aim called terrorism. Cyber terrorism, however, continues to be a significant phenomenon and a lot of discussion about its exact sense, goals, attributes, risk factors and protective methods. Cyber terrorism and cybercrime are sometimes used synonymously, or cyber terrorism may be used to cover cyber-terrorism, blurring the difference among them, notably for the wider populace (Seissa et al., 2017) [6]. Cyber attacks continue to be listed as one of the highest priority global threats to national security. Cyber-attack, whether it happens as a confrontation between nations, as a terrorist or as a criminal act, is an attack in cyberspace aimed at breaching a computer system or network but also at breaching physical systems as was the case with the Stuxnet worm. In both terrorist and military purposes, the same tactics of a hacker attack are implemented. (Duic et al., 2017) [7] break cyber-attacks into phases which they find to be basically the same as traditional criminal offense phases:

1. The very first phase of an attack is to search potential victims. By monitoring the execution of normal target operations, valuable knowledge that is collected and calculated through the applications and hardware used;
2. The second stage of the assault is one of intrusion. There isn't anything that can be done against the target before the attacker gets into the network apart from preventing the availability or connections to those services offered by the target;
3. The next move is to describe and disseminating internal incentives by an overview of the tools and the right of access to the system's restricted and essential parts;
4. The intruder does system damage in the fourth phase or steals certain data;

In addition, they suggest that cyber attacks today mainly consist of:

1. Malware via internet browser attachments, e-mail or other vulnerabilities of the system;
2. DoS to restrict the usage of computers and networking systems;
3. Deletion or transfer (leaving a message) for propaganda purposes to government and commercial websites or to interrupt the informing;
4. Unauthorized intrusion into networks for theft of sensitive and/or proprietary information, Misuse of information collected/use of channel to start attacks on other networks.

Cyber risks definitely redefine such words under these transformational conditions and contrasting perceptions and understandings of security in general and international security. A new global The information security ideology will have to be built in line with the proposals to boost security on the one side, and the existence of cyber threats and motives of actors who initiate them on the other side (Durand & Wegener, 2020) [8].

More than 80 percent of total trading transactions are conducted online today, and this sector has demanded a high level of protection for open and best transactions. The scope of Cyber Security not only extends to the security of enterprise-wide IT systems, yet even to the bigger digital networks they depend on, including cyber space itself and critical infrastructures (M. Wu et al., 2017) [9]. Cyber security plays a major role both in IT development and Internet services. Improving cyber security and securing sensitive information infrastructures are crucial to the protection and economic well-being of each country. Society has become dependent on cyber systems across the entire spectrum of human activities, including trade, banking, energy, health care, communications, entertainment, and national security (H. T. Nguyen & Franke, 2012) [10]. Recent research results also show that the degree of worldwide awareness since 2006 for data security and personal information has increased. Internet viewers are scared of giving away plenty of personal information and prefer to be resisted because there is no real need to maintain their personal information. Cyber security depends on the precautions conservatives take and make important decisions on the choices they make when setting up, maintaining & using the machines and the Internet. Cyber-security includes physical defence of personal information and technology tools (both hardware and software) from unauthorized access obtained by technical means. Albert Einstein was quoted as saying-Problems with the same degree of consciousness that produced them cannot be solved (Zamani, Mahdi Movahedi, 2015) [11]. The issue of end-user errors cannot be solved by incorporating more technology; it must be solved with a concerted initiative and collaboration between the group of interest in information technology as well as the general business community along with vital support from top management.

2. OVERVIEW OF CYBER ATTACKS :

Cyber security is a rapidly growing field that needs a lot of attention due to remarkable developments in IoT networks, cloud and web technology, mobile world, online banking, smart grid, etc. Cloud is becoming more appealing to hackers due to its open nature and the quantity of traffic created by the cloud. For example, the most prevalent cybercrime attacks after data theft are distributed denial of service (DDoS) attacks. TCP and/or UDP flood attacks can drain cloud resources, absorb much of their bandwidth, and damage a complete cloud project in a short time (Hoque, Sazzadul Mukit, 2012) [3]. These security threats include the creation and deployment of an efficient intrusion program that will protect the cloud from zero-day attacks that have just arisen. The most common challenges traditional methods face is that IDS generates false alarms and does not use appropriate standards or parameters to assess threats. This may contribute to the problem of misuse.

Faster transition of data made the network an Interesting and allow access goal for attackers to hack and play with different kinds of attacks. Consequently, many intrusion detection strategies have developed to secure distributed services in the cloud by detecting the various forms of attack on the network (G. Kim et al., 2014) [12]. The big benefit for the population of attackers today is the availability of open access to infrastructure and broad file and knowledge sharing networks. And so, each other day they prepare more and more new kinds of attacks. Software manufacturers who don't pay enough attention to their security modules create vulnerabilities not just to their device but also to the overall system and often become vulnerable to one malicious application for the entire network(Borkar et al., 2018) [13].

3. RESEARCH OBJECTIVE AND METHODOLOGY :

Cyber Security ensures the confidentiality of computer-connected systems, software, hardware and information from cyber attacks. Without a protection policy in line, attacker can easily access your system and misuse your private information, customer data, business intelligence and much more. This analysis is being carried out with the aim of properly understanding the definition of cybercrime and cyber protection and of providing effective and appropriate remedies to address these concerns in today's Internet world. In addition to this, the purpose of the study is to provide a framework for new opportunities for analysis. The following tools are important for the achievement of the desired objective:

1. What are the different types of cyber attacks?
2. What are the various aspects of a targeted cyber attack?
3. What are the various perspectives to Cyber Attack Detection?
4. What are the theoretical constructs of the Cyber Security System?
5. What are the different approaches to predict and avoid network attacks using machine learning algorithms?
6. What are the specific issues of a developer to mitigate cyber attacks?
7. What are the benefits of avoiding cyber-attacks?
8. What are the various works done in the field of cyber security in order to prevent cyber attacks?

4. LITERATURE REVIEW :

There have been a large number of studies in the literature on the issue of cyber security. For general information security strategies, there are diverse common approaches. We've concentrated on using artificial intelligence and machine learning approaches to cyber security issues in this segment.

(Chowdhury et al., 2017) [14] suggested a new method of botnet detection, node-based topology within a network. The technique suggested would be able to detect anomaly by looking for a small number of nodes. This methodology is based on a clustering of self-organizing maps (SOM), which is part of a family of unsupervised system. This analysis used CTU-13 databases, the largest dataset containing nodes labelled with bot. This analysis also used another detection algorithm, supporting the vector machine (SVM), for comparison.

(Neethu B, 2014) [5] Represents PCA architecture for the Naive Bayes collection of features to build a network intrusion detection program. KDDCup 1999 benchmark data collection for intrusion detection is chosen for experiments in this study. The findings demonstrate that the technique efficiency achieves a higher detection rate, less time consuming and has a low cost factor compared to the approach focused on neural network and tree algorithms. Moreover, the proposed program has an accuracy of around 94 per cent.

(Kozik et al., 2014) [15] Proposed a new method for identification web applications targeting cyber-attacks. This The strategy was related to the machine-learning algorithms Naive Bayes, AdaBoost, Part, and J48. Additionally, HTTP Dataset from CSIC 2010 is used to test the proposed model. The study focused specifically on solutions which use HTTP protocols to communicate with servers clients. The authors believed this model could get the higher percentage of detection while getting lower false positive rate. At the same time, the findings have shown that the J48 strategy is the best solution to this problem and about 0.04 is the true-positive value.

(Zamani, Mahdi Movahedi, 2015) [11] reflect different intrusion detection models. These models are divided in this analysis on the basis of classical artificial intelligence (AI) and computational intelligence (CI) such as genetic algorithms and fuzzy logic. They performed various experiments, and compared the efficiency of their algorithms. The findings of the experiment suggest that best results were obtained with decision tree algorithm.

(Hoque, Sazzadul Mukit, 2012) [3] developed a genetic-algorithm-based intrusion detection system (IDS) to accurately detect various types of network intrusion. The proposed model used knowledge evolution theory for filtering the traffic data and thus decreasing the complexity. Alternatively, the KDD99 benchmark dataset was used to test model performance. The experimental results indicate that a fair detection rate has been achieved for this model.

In order to detect the presence of a botnet and identify the bots, (J. Wang & Paschalidis, 2017) [16] suggested a novel approach with two phases. First stage is relevant to the awareness of anomalies by leveraging large differences in an empirical distribution. Additionally, this stage proposes two

Strategies for the creation of empirical distribution. First methodology is flow-based method that estimates the histogram of quantized flows and the latter is a graph-based method that estimates the grade distribution of graphs of node interaction. Second stage uses social network culture in a graph to detect the bots, capturing associations of interactions between nodes over time. They used real-world botnet traffic for the experiments which is a CTU-13 dataset.

(Wijesinghe et al., 2015) [17] concentrate on the identification by examining network traffic flows of a number of families in the botnet. Their method proposed It's in two pieces. Firstly, they identify appropriate dataset models with more specific features to detect botnet from IP flows. Second part used IP flow data to detect unlabeled botnet behaviours. They used publicly accessible IPFIX dataset in this analysis. This technique is a new concept, and has led to botnet detection studies based on IP flow data.

(Haddadi, Fariba Cong, 2015) [18] evaluated various approaches to botnet identification, depending on the model used and the type of data used. Bot Hunter and Snort are two methods focused on public-rule schemes. Other methods are based on Data processing methods, including packet payload and traffic Flow-based strategies. This analysis makes use of five botnet data sets accessible to overall public, such as CAIDA, ISOT etc. Several experiments were conducted using C4.5, KNN (k-nearest neighbours), SVM, and Bayesian networks. Experimental findings indicate flow-based system performance is higher or comparable to the findings published in the literature.

4.1 TYPES OF CYBER ATTACKS

It is necessary to declare this tenderness of virtual vulnerability as the evil result of this rapid leap in technological competence that usually defines this age. This lack in prudent security features that can be described as the debauch misuse of this inherent vulnerability is abused by hackers and some other cyber intrusion. You can illustrate the various types of cyber threats as follows:

1. **Malware -** Malware can be described as a coordinated convergence of cyber and virtual threats of various kinds, and typically consists of Trojan and other similar viruses(Akin et al., 2020)[19]. It can be illustrated as the systematically designed instruction code that usually comes up with the rogue intent to hack the confidential information in the immune set. This also holds the power to demolish the entire collection of knowledge. Malwares typically appear in the virtual scenario coupled with the attachments containing malicious emails, and the consequent download of the attached links that herald vulnerability-related issues.
2. **Phishing attacks -** These assailant kinds typically ask a foreign agent for a reliable metric of information. In addition, often it comes with a request to register in a given connection that was endowed with the previous attachment. On that topic, what can be seen as an efficient index of Virtual intrusion seems to be some of the attachments request personal and sensitive data. In the past few days, this program has developed into a more advanced and elegant version where it allows users to switch to a third interface and eternal intrusions allow them to steal the knowledge accessible from foreign servers and users (Zhang,Ningxia Yuan, 2012) [20]. So, managing their malicious intent has become really simple and useful for the hacker.
3. **Password attacks -** Generally this kind of attacks are characterized by the intruder's intent to break the user's enforced password by merely initiating access to the user's device. Generally, this kind of attacker doesn't add some kind of debauch instructions and malicious codes. In addition, it does not misuse any tools to achieve its goals. In this case, a specific program is typically implemented that violates the prey user's password in a stably guided manner. It normally breaks a user's system's enforced password. There are certain specific program-related applications which possess the ability to initiate brute force attack. This form of program is typically developed and commissioned to crack the target user's password.
4. **DoS Attacks -** Typically, this sort of assailants imparts vehemence to chaos the ideals of a specific Network. In background, the approach by which DoS attacks are inflicted is unique in application since the intruders transmit a deep volume of network signal (Kato & Klyuev, 2014) [21]. This aids congestion network traffic by overloading this. These forms of threats are considerably the most common form of cyber threats as it indulges the user in overcoming the network blockage imposed by the virtual intruder and meanwhile the hacker uses multiple networks to gain access to the preserved information.

5. **MITM attack -** MITM stands for Man in the Middle where the attacker is intending to impersonate the various end nodes within a common service interface and information sharing. These forms of attacks are typically defined and interpreted throughout the Banking sector and financial industries, and are likely to target the online transaction interface. Usually, such attacks earned it access via a non-illusive wireless access node. Since they enjoy this app interchange facility, they have enabled access to all the related metrics of user-owned knowledge.
6. **Malvertising -** In such an attack, the automated attacker pressures the user to compromise with the fixed workstations while adding multiple criminal intent instructions. This malice is likely to occur if the user is prompted to access any questionable advertising index. These were a common practice for potential intruders to upload questionable and malicious material into the celestial system to confuse users and contaminate their collection of information at the same time. Clicking on the infectious connection will move the user to a different third-party interface and grab the confidential text (R. Islam & Abawajy, 2013) [22]. It can be described as a virtual hijack mechanism and the stolen information as a ransom to achieve the cyber security necessary
7. **Eavesdropping -** This can be proven as a virtual overhearing environment where the possible attacker is vulnerable to secretly listening to other private exchanges. This is usually practised among a particular network's diverse and shared hosts. This is not the serious kind of virtual hazard and can be solved by following a few simple acts.
8. **Click jacking** - This kind of assailants typically target the user's normally used virtual interface by simply using some celestial malicious instructions in the form of cryptic codes (Smadi et al., 2015) [23]. Deep down, this process is generally described as a cheap trick from the website of the hacker that makes inexpensive use of tricks and makes the user Click the button with apprehension. To redirect the respective user to another web page, this button is further conditioned. This sort of intruder can also be described as the possible hijackers who are vulnerable to stealing any valuable information from the user's network.

4.2 STAGES OF CYBER-ATTACK

Aimed cyber attacks have no specific pattern of intervention, and therefore there is no chain of events that is absolutely accurate. An assault may be a one-time incident that lasts for minutes, or a segment of ongoing intrusions that extend weeks or even years, taking into account several technological and individual vulnerabilities, like unpatched websites that involuntarily trigger malware downloads, code-injection web servers or browsers that are susceptible to downloading malware-infested mail attachments. Overall, contemplating a targeted phase cyber intrusion is helpful. The targeted attacks occur across several phases:

1. **Reconnaissance -** In the early phase of an attack, an attacker makes use of social manipulation and passivity, Email Phishing, developing a waterhole or perverting removable media to gather information and learn its meaning. The hacker resumes by searching for open-source government or corporate content, scanning, gathering data about targeted networks, their operations, critical staff and targeted mail addresses (Smadi et al., 2015) [23]. To detect vulnerabilities that need to be exploited, the attacker(s) invest some time cataloguing everything they discover to obtain profound insight into what is currently being utilized against the security features of database and the learning system.
2. **Scanning** – The next step will proceed for the hacker to find a low entry point that allows network connectivity; may this be poor judgement, restricted device utilization, perception management victims, lack of security strategy or ignorance. The intruder stealthily combines in with normal traffic if a network is infected within the network, making identification increasingly hard. The attacker then starts by covertly implementing their cyber tools to isolate weaknesses in the protection within critical network connections (Duic et al., 2017) [7]. The tracking system will search the systems probing area, searching for weaknesses to generate a server elevation cyber graph. This may be the move be done via resources that can be found conveniently across the network. Searching for weaknesses is typically a long process and, regardless of how big the network is, it can take months.
3. **Arbitrary code execution** – Malicious actors may remotely build unauthorized network adapters or configuration issues on your device to install malicious programs such as Remote Access Trojans

(RAT), root kits, and insert keystroke authentication software to acquire credentials for higher authorized access on the network, and also get passwords that will allow them to access all areas of the device. The intruder begins expanding after obtaining a set of appropriate systems on the preservation of the impact.

4. **Access and Escalation** – Now as the hacker has attained unrestricted control of the target system, they may try to push for lateral expansion and establish a strong presence. Many attackers hide in the Network's darkest regions, and stay inactive as they try to come and go. Some will choose to buckle across the network and identify the important parts they are hunting for genuine to accomplish their goal, such as sensitive information, private information, property rights or computer communications mechanisms that degrade or disrupt network activity at will.
5. **Data Collection, Exfiltration, and Exploitation** - The reputation of the network has been greatly undermined by this point. Once an intruder thinks they have gained safe access to the system, they can now alter or transfer confidential data to any spot they wish. The attacker may use or leak the stolen data with third parties or even the Internet for more targeted hackers (Zahid et al., 2020) [24]. The ultimate goal of their mission is achieved and it is typically too hard for the breached enterprise to defend itself by this time.
6. **Clean up** – Not all attackers take the final step, some merely detach, and unworried about the victim possibly finding out just what happened or choosing to leave underneath a calling card to make a fuss about their achievement. Highly qualified attackers attempt to remove any forensic evidence that suggests a violation in all network systems (Seissa et al., 2017) [6]. They can erase / overwrite documents, erase embedded data, clear log files, disable alarms, roll back up software upgrades, unplug backups or erase hard disks. They would do their utmost to mask or delete any signs that the accident has ever happened, making it appear as a code error left behind secret backdoors anywhere they want to go back to, or breaching the systems further.

4.3 ARCHITECTURE OF CYBER ATTACK DETECTION SYSTEM

Safety is a necessary aspect of rising network infrastructure nowadays by increasing network systems. Network IDS provide a defence model for all hazardous security threats to any network (Aburrous et al., 2010) [25]. The IDS could detect and block network traffic relevant to the attack. Control of network is a complex model. Implementing IDS may cause network delays. Many network IDS centred on software are being developed. Yet the model has a high-speed traffic problem. Application architecture offers an overview of software modules, relation between each component and software application high-level design (Zamani, Mahdi Movahedi, 2015) [11]. Although these systems are very different in the techniques that each system implements, they also gather information and analyze it. The majority of these systems rely on the infrastructure of popular architecture (as shown in figure 1). The following fundamental architectural components are as outlined below (Axelsson, 2015) [26]:-

1. The processing of data is responsible for gathering information from the grid as well as the machines being tested.
2. Detector ID algorithm builds sensor information to detect suspicious attack incidents.
3. Knowledge base contains information obtained by sensors; this is accomplished by structured input, input profiles, etc. in pre-processed format. A security expert or network expert often delivers that data.
4. Configuration device provides the latest Intrusion Detection Systems status data.
5. The solution part starts with a discovery of an attack. These responses could be programmed either as active or may include a human interaction also called inactive.

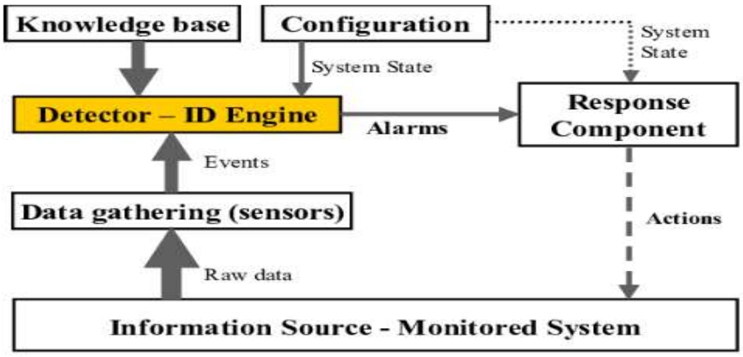

Fig. 1: Shows a popular Intrusion Detection Device design structure (Axelsson, 2015) [26].

4.4 APPROACHES FOR ATTACK DETECTION

Machine learning and evolutionary algorithms can typically be used to identify and forecast attacks, as well as statistical methods and correlation rules. Similarly, most solutions to mitigation of attacks are done by the study of traffic to detect and drop (or block) a malicious operation (Ibor et al., 2018) [27]. That is shown in Figure 2.

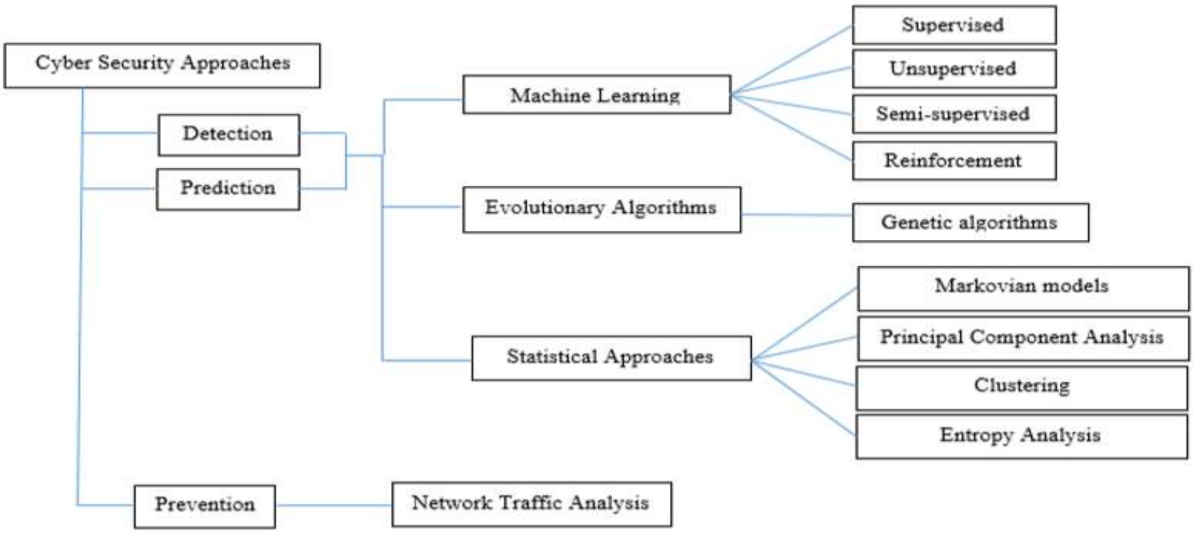

Fig. 2: Summary of Cyber Security Approaches (Ibor et al., 2018) [27].

Detection of cyber-attacks is a growing strategy for preventing a threat. To announce the presence of an attack pattern or profile in a network, it includes reacting to an unexpected contact. Intrusion prevention is one of the core techniques for identifying cyber-attacks. Intruder detection is, according to (Aissa & Guerroumi, 2016) [28], the method of detecting an intruder or an characteristic attack in a continuous flow of connections. Detection of intrusion occurs with the use of intrusion detection systems.

Systems for detecting intrusion are divided into three strategies. These include approaches to abuse (signature-based), anomaly, and hybrid detection, respectively. Although identification of abuse utilizes the signatures of documented attacks to help identify intrusions, identification of anomalies uses profiles of regular network behaviour to report intrusions when a change from the usual profile is detected. Combining the two approaches produces a hybrid approach (G. Kim et al., 2014) [12].

Several studies are published in public view about cyber-attack identification. Some of these methods, though, have been relatively ineffective in identifying attacks although others have resulted in high computational resources usage. Likewise, much of the methods proposed in the current literature are computationally infeasible and can only survive as masterpieces of science. Subsequent articles will address more public domain solutions to cyber-attack identification, as well as demonstrate the technique, strengths and limitations of each strategy.

4.4.1 DETECTION BY MACHINE LEARNING APPROACH

Machine learning methods have been introduced in recent decades become common in detecting cyber-attacks. Machine learning is especially efficient in evaluating data and predicting the outcome of such events based on the sample inputs available which are used to create an acceptable model for making the right decisions. The key tasks of machine learning algorithms are to use training data to identify and predict the existence or absence of an acquired case (Azab et al., 2016) [29]. The use of machine learning in the latest prevention of cyber-attacks environment has helped boost the method of identification to a strong stage of precision. In this paper four kinds of machine learning techniques are discussed. These include methods of controlled, unmonitored, semi-supervised and validated instruction.

4.4.1.1 SUPERVISED LEARNING APPROACH:

Supervised learning is a component of pattern recognition that uses a collection of named instances known to be training data with the target output correspondingly. A statistic system for categorizing new data sources throughout the training phase is generated from the named instances. This is done through injecting a certain machine-learning algorithm into the named instances. Some of these approaches to machine learning as illustrated in (Buczak, Anna L. Guven, 2016) [2] include decision trees such as C4.5 and ID3 algorithms, Artificial Neural Network, Hidden Markov Model (HMM), Support Vector Machine (SVM), K-Nearest Neighbour (KNN), and Naïve Bayes.

Web pages are one part of cyberspace that's vulnerable to malicious attacks. With an ever-expanding web footprint in all application types, with the increasing use of web pages material for practices such as social media communications, online banking, e-commerce, e-government, and many others, the need for an efficient approach to identifying fraudulent web pages cannot be overemphasized.

The ability to quickly alter the source code of web pages by adding malicious code as observed today that contributed to a different category of malicious websites that could intensify the environment of assault and mislead users into revealing sensitive personal data. To this end, (Huseynov et al., 2014) [30] Drew up a digital approach for the identification of fake web sites which use methods to abuse and analysis of anomalies. The hybrid malicious web page detection technique hierarchically combines the violation and identification of anomalies modules so that abuse detected module analyzes every web page at first instance. This system often makes use of the algorithm of the decision tree to identify misleading web sites by contrast the properties of those Pages of established trends on web page. When the first stage is complete, the unclassified pages are fed into the anomaly detection system to detect new instances of malicious pages with the aid of one-class SVM.

With the integrated solution focused on the use of both the intrusion and anomaly detection Ways of preventing network threats, efficiency was strengthened with a decrease in time complexity, resulting in a higher identification accuracy of up to 98.2% and low level of false warning of 1.7%. In this case, the using algorithm for decision tree for forecasting instances comes with its own drawbacks. Decision trees may be unreliable if the exact information is not used, and as such a small shift in the input data may result in major tree changes. It is not suitable for identifying intrusions as the resulting diagnosis may be completely inaccurate with disastrous implications for vital network infrastructure. A 3-step method is laid out in (Lin et al., 2015) [31] for the realization of a novel feature representation strategy based on CANN approaches. This method incorporates two estimated and combined distances, which represent the distance between the database and cluster core in the first case, while the second range in same class is determined in terms of the data point and its closest neighbours.

Using the classifier k-Nearest Neighbour (kNN), the resulting one-dimensional distance-based feature It used for presentation each data point throughout the sample field chosen to achieve attack detection. A clustering algorithm is used initial state to remove cluster centres, and the number of training samples from testing set is indeed a feature of a group number. In the second level, A new feature on component is generated to represent a data point by calculating and summing the distances in two dimensions viz-a-viz between the data points in the dataset and the cluster centres, as well as an individual data point in a related cluster and its closest neighbours. Finally, to devise new data is the retrieval of cluster centres and closest neighbours. The k-NN classifier is learned and evaluated using the combination of assessments and advanced training sets to find new and unknown instances even in string connection. It's been observed in experiment that the CANN solution was efficient with respect to k-NN and SVM classifiers with respect to the six-dimensional data set used, and demonstrated substantially high detection precision with a marginal false positive rate (Bhamare et al., 2017) [32]. Conversely, by evaluating the nineteen dimensions dataset, CANN obtained the same success levels as the k-NN and SVM classifiers. Some of the shortcomings found in the system includes CANN's failure to identify root (u2r) applications, and root to local (r2l) attacks. This may not be unconnected for use of one-dimensional distance-based feature representation to develop and evaluate the framework which will essentially detect the various attack classes. In doing so, the function space is believed not to exhaustively represent the patterns of u2r and r2l attacks. A multiple learning strategy that considers the cluster centre and nearest neighbour approach (CANN) to be enhanced as described in (Lin et al., 2015) [31] is further elaborated in (Shapoorifard & Shamsinejad, 2017) [33]. The technique, dubbed ICANN, deploys two supervised algorithms for machine learning, that is, the classification algorithm k-Means and the algorithm k-Nearest Neighbour.

4.4.1.2 UNSUPERVISED LEARNING APPROACH

Unsupervised learning operates by finding trends used as the training data in an unlabeled dataset to make the correct classification a collection of decisions in different cases. This typically includes clustering to classify the groups that instances belong to. (Song et al., 2013) [34] addressed an anomaly detecting method with an unsupervised learning approach that is capable of dynamically tuning and maximizing the value of parameters to arrive at better categorized instances that either represents an attack string or a usual link. The proposed approach implements after-the-training sorting of cases, which involves such phrases as sampling, clustering, and modelling. Filtering achieves the necessary normal data sub-set, which is then partitioned into clusters k. Such k clusters reflect standard traffic data patterns, such as HTTP, FTP, and SMTP. The one class SVM is used for the generation of k SVM models also called k hyper spheres for classification for each regular cluster (Zarca et al., 2020) [35]. k model is then paired with new instances to decide whether such an existing case inside the predefined hyper sphere, in which case it is a natural relation, then the state of attack is flagged up.

Usage of unsupervised way of learning offers an efficient strategy for classifying new instances using the threshold at the time of model building to distinguish normal and attack results. A major downside of the strategy can be clearly established at this point, based on the assumption that typical links differ on heterogeneous networks, and as such building profiles of normal activity will dramatically deteriorate. This major variation in one network's behavioural patterns and characteristics from other networks will result in an inconsistent model that will inevitably require an effective assessment of the tuning parameters and adaptation to satisfy the needs of a given network setting. A fixed-width clustering algorithm generates clusters in function space at the point of training the construct. Anomalous clusters are known if there are fewer training traffic samples than a given threshold on these samples. In comparison, in the testing stage, matching a specific traffic sample to a cluster processing is carried out to confirm an anomalous trend of life or not (Ravikumar & Govindarasu, 2020) [36]. The major downside to this approach is the intense demands for computing sensor nodes that can contribute to large overheads on host network.

4.4.1.3 SEMI-SUPERVISED LEARNING APPROACH

(Ashfaq et al., 2017) [37] suggest that semi-supervised learning takes into account all labelled and unlabeled samples for a proper classification. Similarly, (Aissa & Guerroumi, 2016) [28] states that using a pre-labelled sample, semi-supervised machine learning methods models human behaviour. Semi-supervised learning then incorporates the influence of both supervised and unsupervised in-process of learning methods of creating a model for classification of new instances of a dataset. Additionally, (Aissa & Guerroumi, 2016) [28] suggested a two-stage semi-supervised computational method for identifying abnormalities in the network. The methodology uses prelabelled typical instances to construct a probabilistic model. The formula is then used using a fixed criterion to measure variance from normal behaviour. The second stage uses an iterative method to reduce the false rate, which boosts the resemblance gap and dispersion rate of the probabilistic model's initial classifications (Aissa & Guerroumi, 2016) [28]. (Han et al., 2016) [38] suggested a semi-supervised learning approach in cloud-based systems as a countermeasure for co-resident attacks. The remedy has established a framework for defence which makes it computationally costly for co-resident intrusion is being successful on a virtual environment with a cloud computing environment. The problem was modelled with users categorized using clustering analysis and semi-supervised SVMs as a 2-player safety game (Xie et al., 2014) [39]. Users are regarded in accordance with the adjustment in the method of virtual machine allocation as high risk (malicious), medium risk (uncertain) and low risk (legal). It helps the defence system increase the potential cost of an attacker to accomplish a computationally costly method of attack. The method achieved progress by raising the attacker's overall expense to two orders of magnitude as a countermeasure for attacks on co-residence. Nonetheless, in practice it is not easy to have a single datacenter to using the describe method the various situations of multiple datacenters that are likely to accommodate colocation and co-resident attacks.

4.4.1.4 REINFORCEMENT LEARNING APPROACH

Reinforcement learning is a machine learning technique that enables the learning of a software entity like a sensor node by experience with its surroundings. (Alsheikh et al., 2014) [40] claims that trying to improve learning is key in the sense of pattern recognition since it makes software agents to construct experiences from their encounters with the world in order to take the right long-term rewards behaviour. Similarly, (Xu et al., 2014) [41] stated that reinforcement learning agents transfer messages in an initially unknown context and use the acquired knowledge to redefine policies of action to increase their rewards. The authors suggest that reinforcement learning is appropriate for solving sequential problems that can be modelled as Markov decision processes (MDPs) and as such appropriate for understanding problems with learning power. Supervised learning algorithms typically find these questions impossible to understand.

(Shamshirband et al., 2014) [42] used Fuzzy Q-learning to detect and avoid WSN intrusions. To predict DDoS attacks, the technique utilizes a mixture of cooperative game theory and fuzzy Q-learning algorithms. For a 3-player strategy game, the solution models sinkholes, a base station and an intruder and the machine is triggered when a torrent of packets is aimed at the target node. At this level, the received packets are calculated against a common alarm event threshold in WSN and the solution applies cooperative security countermeasures for the sink hole and base station if such a threshold is breached. For performance assessment, low-energy adaptive clustering hierarchy (LEACH) was simulated with NS-2 simulator to demonstrate the approach's accuracy in detection and defence. The solution architecture allows the sink hole and base station to react to a random attack while selecting the most appropriate technique to detect and respond. To predict potential attacks, the IDPS amends the learning criteria regularly in a process described as lifetime self-learning of past attacks using fuzzy Q-learning (Xia et al., 2010) [43]. With the method considering DDoS just fights the flooding, its effectiveness against other types of attempts can be hard to find out. The model therefore requires a holistic improvement to effect enhanced decision-making capabilities, particularly with regard to truncating novel attacks.

4.4.2 DETECTION BY GENETIC ALGORITHMS APPROACH

Genetic algorithms (GAs) are a hybrid part of evolutionary algorithms (EAs), effectively meta heuristics described by the natural selection mechanism. A genetic algorithms' most critical role is rooted in generating optimization solutions and searching problems based on such bio-inspired operators as mutation, crossover, and pick. Accordingly, (Hoque,Sazzadul Mukit, 2012) [3] suggested an intrusion prevention method focused predominantly on the use of genetic algorithms. In order to minimize the complexity attributable to classification, the genetic algorithm approach is tuned to detect various forms of attacks based on evolution theory to information evolution with a consequence filtering the captured traffic data. The approach's efficacy was assessed using three variables, which include fitness function, individual representation, and GA parameters. In the proposed solution, two specific functions are applied to attain the purpose of the algorithm. These include the pre-calculation and identification processes. The training data were present in the pre-calculation process to construct a collection of chromosomes and is used in the next shift for comparisons. Detection is accomplished in the second stage by constructing a population to evaluate the method and ultimately the test data is estimated using certain measurement processes such as discovery, convergence, and mutation. A fitness function then determines the fitness of the sample population for every chromosome. Experimental Experiments showed that the approach is worked well against different intrusion types including test, Root to Local (R2L), Denial of Service (DoS) and User to Root (U2R) attacks. Measuring a chromosome's fitness with the standard deviation equation with distance restricted the approach's efficiency with respect to identification and false positive frequency. For this respect the use of a more effective heuristic may be very useful for a better detection method.

(Rastegari et al., 2015) [44] Proposed creating statistical guidelines for identification of attacks. The system relies on necessity to closely examine data about internet traffic in order to directly identify unwanted traffic using a genetic algorithm due to the similarities between regular and attack patterns. Using statistical continuously valued input data, the algorithm is optimized to develop simple interval dependent laws. Then, each rule is assessed using a fitness function in conjunction with a new individual representation. During the learning process improved rule sets are created in this way. Then, the rules produced are used to identify the data points. The chromosome configuration is formulated according to pattern to follow rules with a mutable feature set and fitness mechanism that is capable of rewarding inter-rule cooperation. This also includes a mechanism to assess the degree of exclusivity at the selection stage in an adaptive manner to generate succinct rule sets. During the pre- processing phase, setting data normalization is done to generate normal and crime records for training and evaluating the emerging rule-based classifier. Pre-processing often calls an optional stage of selection of features that functions to provide seed rules for the initial population of rules. This is accompanied by the assessment step, where a conventional fitness system evaluates component rules while a higher-level system selects rule sets that operate in the detection process together.

One major strength of the proposed approach is the non-dependence of packet header category features like destination and origin IP addresses(Huang & Zhu, 2019) [45]. This means that the method leverages network traffic statistical capabilities to detect any unusual activity present in the traffic stream, and as such is ideal for detecting novel attacks. Similarly, the use of concise rule sets, that are analyzed through the genetic algorithm and identified to comply when specifically covering the quest field, leaves the rule sets small and effective in detecting proven and novel assaults. Considering the number of rule sets included within the regular grouping and attack cases, likewise the metrics of fitness and efficiency, it is important to consider miniature limit values shift. Unfortunately, the current model is oblivious to these improvements because no testing models are nearby making it unable to execute and classify the type of intrusion that infiltrates a network even at this given point in time in a multi-class scenario.

4.5 ADVANTAGES & CHALLENGES OF CYBER ATTACK PREVENTION

As every other living room, the system has its own advantages and challenges. Though it improves the life of a man in almost all ways, be it education, housing, connectivity, smart cities etc. There are different obstacles that we must address so as not to turn technology into our own enemy. Cyber security faces a greater challenge than any other technology continuum. Cyber criminals have also begun to misuse technology-controlled tools to accelerate cyber-crimes like fraud and robbery (S. N. Islam et al., 2018) [46]. With security protocols still being developed and developing driven steadily, these cyber-attacks are very difficult to prevent.

Advantages:

1. Networks, computers and documents are protected from unauthorized access.
2. Protection of Important Data – Knowledge is one of the enterprise's most valuable properties. Its Protection is key aspect of the structure in information technologies. Integrating a security solution can provide protection for all information.
3. Stay ahead of Competitors – Implementing Security Strategies in competition puts company competitive. IT Protection System blends with enterprise systems that already exist. Protecting data acts like icing on the cake.
4. This builds strong credibility and profile. Improved confidence among stakeholders in the security arrangements for your information.
5. Faster recovery times should a disruption occur. It guarantees that vital market activities proceed in the event of natural disasters or high-impact health accidents.
6. It ensures laws and regulations are adhered to. Improved company credentials with proper safety checks in place.
7. Improved security of knowledge and maintenance of company continuity.

Challenges:

1. **Ransomware Evolution:** Ransomware is a form of Ransomware that locks the data on a victim's device, and demands payment before the ransomed data is released. Connection rights restored to the survivor, following positive payment. Ransomware is the bane of data professionals, cyber

security, information technology and executives. Ransomware attacks in cybercrime areas are on the rise day by day. To defend the company, IT practitioners and corporate owners need a strong response plan against Ransomware attacks (Zimba et al., 2018) [47]. It requires careful preparation to retrieve data and service from companies and consumers, as well as reporting any violations against the Notifiable Data Breaches program.

2. **Block chain Revolution:** Block chain technology is the most important technological invention for the time span. It is the first time we already have a perfect one native digital medium in human history for peer-to - peer exchange of value. The block chain is a system that makes for crypto currencies such as Bitcoin. The block chain is a vast global platform that allows two or more parties to make a transaction or do business without needing a trusted third party (Narang et al., 2014) [48]. With regard to cyber security, it is difficult to predict what block chain systems will offer.
3. **IoT Threats:** IoT is an interrelated network of physical devices that can be connected via the Internet. The linked hardware devices have a unique identifier (UID) and are able to transmit data over a network without any human-to - human or computer-to-computer interface criteria (Duic et al.,2017) [7]. The firmware and software running on IoT devices makes consumers and companies highly vulnerable to cyber-attacks. While planning IoT stuff, the use of cyber security and for commercial purposes is not kept in mind.
4. **AI Expansion:** AI's primary advantage in our information defence approach is the opportunity to secure and defend an infrastructure before the malware attack begins, thus minimizing the effect. In a moment when a threat impacts a business, AI takes immediate action against the malicious attacks. IT business leaders and information security management teams view AI as a future protective control that will allow our company to stay ahead of the cyber security development curve.
5. **Serverless Apps Vulnerability:** Serverless software and apps are applications that rely on third party cloud storage or back-end services such as Google Cloud feature, Amazon Web Services (AWS) lambda, and so on. The serverless applications allow cyber criminals to quickly distribute attacks on their network as the users access the software on their computer locally or off-server. The serverless applications do little to keep out our data from the attackers. The serverless technology does not help if an attacker achieves access to our data by vulnerability such as leaked passwords, a compromised insider or then serverless by some other way (Barraclough et al., 2013) [49]. Typically, the applications without servers are small in size. It helps developers get their applications started fast and easily. They don't need to think about the network that underlies them. The web-services and data processing software are the most popular serverless applications.

4.6 SUMMARY OF RELATED WORK

Table1: Review of findings from 2010-2020 presented by various authors.

Sl. No.	Author(s)	Year	Inventions/Findings/Results
1	Aburrous et al. [25]	2010	Proposed a distinctive phishing website solution using Data Mining and Fuzzy logic combination to save Internet users when performing online purchases.
2	Coskun et al. [50]	2010	Propose a tool used by shared contacts to identify local members of an unstructured botnet.
3	Xia et al. [43]	2010	Developed A scheme for detecting a DDoS flood attack using blurred logic
4	Wang et al. [51]	2010	Design a peer-to - peer hybrid botnet that consists of servant and client bots.
5	S. X. Wu & Banzhaf [52]	2010	Focused on Computational Intelligence approaches and intrusion detection applications.
6	Nappa et al. [53]	2010	Recommend a parasitic botnet protocol that exploits Skype network overlays.
7	Zhong & Yue [54]	2010	Uses fuzzy c-means and Apriori techniques to construct a model and detect unknown attacks on the DDoS.

8	H. V. Nguyen & Choi [55]	2010	Detects only known attacks by using k-nearest neighbour technique
9	Xiang et al. [56]	2011	Detects DDoS flooding attacks effectively using new data metrics
10	Fedynyshyn et al. [57]	2011	Suggested a solution for using persistence to identify and classify C&C channels into their architecture (HTTP, IRC, or P2P) by monitoring the traffic of individual host.
11	Saad, Sherif traore,issa ghorbani [58]	2011	A comparison was made between five machine learning techniques commonly used for the detection of decentralized botnets.
12	Zhang et al. [59]	2011	Propose a botnet P2P communication technique by finger-printing malicious and benign traffic.
13	Y. Wu [60]	2011	Used the decision tree and traceback for offender location using corresponding traffic flow patterns
14	Raj Kumar & Selvakumar [61]	2011	RBPBoost combines an ensemble of classifier outputs and a cost minimization strategy for Neyman Pearson to make a final classification decision during DDoS attack detection and get a high DR
15	Karimazad & Faraahi [62]	2011	Uses neural RBF networks and achieves weak FAR
16	Udhayan & Hamsapriya [63]	2011	Uses an SSM to identify DDoS attacks within consecutive time intervals based on sampling of flow
17	Sa, n.d.[64]	2011	Proposed an agent-based model for the classification of normal and attack activities in each topology cluster, using two-tier hierarchical network topology
18	Zang et al. [65]	2011	Suggested hierarchical and k-mean clustering for the detection of C&C botnets.
19	Gupta et al. [66]	2012	Uses an ANN to predict zombie numbers in a DDoS attack
20	Garasia et al. [67]	2012	By applying four main phases called traffic representation, separation filtering, and detection, the Apriori association algorithm used to identify the presence of a C&C channel for HTTP botnets.
21	Jeyanthi & Sriman Narayana Iyengar [68]	2012	Detects attacks by DDoS by entropy-based analysis
22	François et al. [69]	2012	A technique for detecting complete DDoS flooding attack. Supports even gradual deployment on actual networks
23	H. T. Nguyen & Franke [10]	2012	Proposed System for Adaptive Intrusion Detection (A-IDS). This model is capable of detecting various types of attacks in heterogeneous and adverse network environments.
24	Zhang and Yuan [20]	2012	Proposed phishing detection approach which makes use of the neural network as a technique of machine learning.
25	Warriach [70]	2013	Developed an approach by proposing Hidden Markov Models (HMMs) to identify and classify data and system fault types.
26	Lee & Kim [71]	2013	Exploring the design and mitigation of botnets using URL Shortening Services (USS) for alias fluxing.
27	Zhao et al. [72]	2013	Addressed the ability to detect botnet traffic by tracking a small portion of the flow and by creating a classifier on identified botnets to identify unknown botnets.
28	R. Islam & Abawajy [22]	2013	Proposed an exclusive Multi-Tier Classification Model approach along with the method of extracting phishing

			email features weighing the contents of the text and message header and selecting feature by priority level.
29	Barraclough et al. [49]	2013	Innovative approach to phishing attack identification and effective countermeasures; Neuro-Fuzzy Logic with five inputs.
30	Sharma & Parihar [73]	2013	Used SVM classifier for wormhole detection, black hole and selective forwarding attacks.
31	Louvieris et al. [74]	2013	Proposed an effect-based IDS function identifier using Naive Bayes as a selection tool.
32	Kaur, Gursheen Singh [75]	2014	The behavioural shift of sensor nodes was analyzed using data mining techniques and mechanisms were developed to classify variable black holes.
33	Xie et al. [39]	2014	A novel anomaly detection system using the Support Vector Machine (SVM) and ADFA-LD is proposed for experimentation
34	Kato & Klyuev [21]	2014	Analyzed a large number of network traffic packets and used the patterns of DDoS attacks for each IP address to implement a DDoS attack detection program.
35	Huseynov et al. [30]	2014	Comparison of K-means algorithm with Ant Colony System algorithm to detect decentralized botnets.
36	Shamshirband et al. [42]	2014	Fuzzy Q-learning (FQL) approach used to detect flooding attacks.
37	Stevanovic & Pedersen [76]	2014	Built a new botnet detection method focused on flow-level network traffic analysis, and supervised MLAs to catch malicious botnet traffic patterns.
38	Narang et al. [48]	2014	Instead of a conventional 5-tuple flow-based detection approach, a 2-tuple conversation-based approach, port-oblivious, protocol oblivious and deep packet inspection is not necessary.
39	Smadi et al. [23]	2015	Proposed a data mining algorithm-based phishing detection model using features extracted from various sections of emails.
40	Rao & Ali [77]	2015	Suggest a solution to phishing attacks by suggesting a combination of whitelist and tactics focused on visual similarity.
41	Wijesinghe et al. [17]	2015	Proposed traffic analysis techniques use fixed IP flows in various products and IPFIX to build a standardized framework for detecting a variety of bot families.
42	Bhuyan et al. [78]	2015	Suggested an empirical analysis using various knowledge metrics to resolve critical security problems, such as identification of low and high-rates DDoS attacks
43	Hoque et al. [79]	2016	Presented a system to track DDoS attacks utilizing new statistical test called FFSc.
44	Bhamare et al. [32]	2016	Focused on imbalance of huge amounts of research on supervised ML techniques and their applicability to real-time scenarios, and concluded that supervised ML techniques need substantial rework to improve cloud security performance.
45	Azab et al. [29]	2016	Researchers suggested methods to detect C&C channel traffic as DPI, DNS request behaviour, time, correlation and machine learning
46	He et al. [80]	2017	Formulated a machine-learning based DDoS attack detection method to avoid source-side attacks in the cloud.

47	Alejandre et al. [81]	2017	Suggested selection of a set of features for detecting botnets in the C&C phase using the GA as an optimizer algorithm and the C4.5 classification to evaluate individuals in the GA.
48	M. Wu et al. [9]	2017	Physical data machine learning methods for the detection of Cyber Physical attacks in CMS are developed and implemented.
50	Zimba et al. [47]	2018	Modelled various multi-stage crypto Ransomware attacks emanating from various sources of CI infiltration and validated with WannaCry attacks.
51	Islam et al. [46]	2018	Investigated the effect of the EMS attacker's false data injections while optimizing the attack signal to gain full benefits from legitimate participants while preserving the supply-demand balance on the local energy market.
52	Kim & Park [82]	2018	Proposed an FPGA-based Network Intrusion Detection System (NIDS) for IEC 61850 industrial network works designed specifically for substation automation.
53	Ilavendhan & Saruladha [83]	2018	Studied VANET security problems and multiple network layer assaults in VANET
54	Ferreira [84]	2019	Focused on the malicious URL, hackers have various techniques and algorithms to blur their URLs in order to bypass defences.
56	Huang & Zhu [45]	2019	Developed multi-stage incomplete information Bayesian game system with the existence of Advanced Persistent Threats (APTs) to develop proactive and adaptive defence strategies for critical infrastructure networks.
57	Roopak et al. [4]	2019	The CNN+LSTM hybrid model studied performs better than the rest of the machine learning algorithms and deep learning models.
58	Akin et al. [19]	2020	Built a unified software-defined network (SDN) automation solution sufficient to prevent cyber-attacks at the root of the attack
59	Zahid et al. [24]	2020	A mitigation mechanism was developed to reduce risks on the application layer related to authentication, data integrity, data freshness, confidentiality, and non-repudiation.
60	Ravikumar & Govindarasu [36]	2020	Proposed identification of anomalies using Machine Learning and model based mitigation to ensure secure and robust operation of the WADC system.
61	Zarca et al. [35]	2020	Set out a novel solution for managing dynamically virtual IoT HoneyNets to mitigate cyber attacks in IoT networks enabled by SDN / NFV.
62	Durand & Wegener [8]	2020	Analysed how cyber threats could be carried out be avoided from security and a profit / production perspective causing problems for a chemical company.

5. DISCUSSION :

Increased dependence on information technology and the internet of things makes it important that IT professionals are alert to growing cases of cyber attacks with the sole purpose of being proactive in order to react as rapidly as possible when IT infrastructure is under attack and also introduce mitigation measures to avoid more attacks(Ferreira, 2019)[84]. One of cyber security's most problematic elements is the rapidly and constantly evolving nature of the security risks. Cyber-criminals evolve their hacking techniques rapidly. We strike rapidly, making defence more important than ever before in due time.

Consequently, having an awareness of the threat is one of the first steps involved in implementing a successful information security strategy.

Cybercriminals today use many sophisticated methods to escape detection as they hack into corporate networks to steal intellectual property secretly (Seissa et al., 2017) [6]. They also encode their threats using complicated algorithms to avoid detection by intrusion prevention systems. If a target has been broken, attackers may attempt to download and install malware onto the compromised device. In many cases the malware used is a newly evolved version that is not yet exposed to conventional anti-virus solutions. The development of Ids is the best way to secure devices and networks for the detection of intruders (S. X. Wu & Banzhaf, 2010) [52]. Hence IDS 'role was not just that to detect intruders but also to track intruders attack. A specific framework shall be drawn up to protect data and services from unauthorized access, harm and denial of use. The security perspective should be prepared for any system based on the expected results.

6. RESEARCH GAP :

Some of the concerns we found about the study gap are:

Research gap 1: Data mining techniques to enable intrusion prevention are being developed for cyber analytics. Techniques used before like a firewall, and IDS failed to identify, without his knowledge, the real-time attackers that occurred in the manager's absence. Recognizing the attacker in real time is difficult, because it can create multiple IP and packet attacks. A computer network is a combination of Software and Hardware. Each component carries risks, poor health, and shortfalls. Ransomware attack leaves data unprotected. Those who learn programming and programs can quickly find out from the log files about the different operations being carried out on the systems.

Research gap 2: A framework for detecting intrusion of PS-Poll DOS infiltration in 802.11 networks, application of a distinct system of real-time events. This technique makes use of RTDES to monitor Denial of Service attack in real-time on a single event system. High accuracy and detection rate are one of the major advantages but frame shortages are one of the major disadvantages.

Research gap 3: Network Intrusion Detection (ID) is tackled by unattended and unattended hybrid mining-a detailed ISCX case study. This proposes a detection of hybrid intrusion (kM-RF) which the alternate approach usually outperforms in terms of the false alarm volume, accuracy and detection times. ISCX (a typical intrusion detection dataset) is used to determine the efficacy of kM-RF and an in-depth analysis is conducted to test the effects of any observed pre-processing features or characteristics. It also uses a special pre-treatment approach for categorical transformation methods or numerical data attributes and generates more raw data segregated classes. Some new features or applications to find payloads, clustered attacks and IP scans and a mix of kMeans and random forest classifiers to prevent further interference effectively.

Research gap 4: The approach involves a technique for solving the problem of malicious attack detection by reviewing the online data sets. This is done by the use of a Bayesian classifier which is incrementally naive. In comparison, active learning allows the problem to be solved by using a limited collection of specified data points, which are also very costly to obtain.

Research gap 5: Deep learning that can create better and more effective intrusion detection architecture is used. The aim approach is to distinguish normal behaviour from anomalous activity in the network. The IDS (Intrusion Detection System) is one of the methods used to detect unwanted network or device activity and protecting the machine from network attacks. Attacks are observed in the system by distinguishing between actions and functionality of the rising and irregular networks. This work also defines numerous methods used in experimental analysis to produce IDS.

Research gap 6: The constant introduction of new and emerging threats targets and challenges a wide range of companies around the world. For this reason, the scientific community has drawn attention to the existence and improvement of the Intrusion Detection Systems efficiency. This is a groundbreaking way of monitoring malicious behaviour in terms of DDoS and Ransomware cyber threats using deep learning techniques. Due to the exponential growth of Mobile apps and their use by most Internet users, cyber security achievement, data protection and safe communication are deemed necessary. At the same time, increased exposure to much more advanced cyber threats has been noticed through the Internet and computer networking in the digital world of academia and industry, with financial costs particularly in Small-Medium Enterprises (SMEs).

Research gap 7: Self using Novel Network Intrusion Prevention Software Organizing an improved neural vector system network with assistance has been proposed. Because of its architecture, the proposed program does not have a secure solution that is neither signed nor based on rules, and is highly effective in minimizing known and unknown risks.

Research gap 8: For multifunctional efficiency, detection accuracy and performance in real time of detecting abnormal activity within industrial networks are effectively increased. The novel apps are dual to quickly pick a node with a high security coefficient as the centre of the cluster and align the multi-function data in a cluster around the centre. Experimental findings indicate that in terms of the detection rate and time compared to other algorithms the suggested algorithm is of high quality. The sensitivity of detecting suspicious data in the networking sector exceeds 97.8%, and the incorrect identification result dropped by 8.8%. Detection devices for intrusion detection can effectively identify and track events involving intruders although it is challenging with network security technologies. The usage of intrusion prevention devices for industrial networks would thus remove the restrictions of traditional network protection methods, thereby perfecting the entire network of industrial safety systems.

7. RESEARCH AGENDA :

1. Which are the best Machine Learning Algorithms to combat cyber attacks?
2. What technology will enhance the privacy of a wide network of users exchanging data?
3. What system can prevent cyber attacks and protect the data over the network?
4. What new development framework can be equipped to integrate a cyber security program with the best use of machine learning algorithms?
5. What Machine Learning Technology can be proposed for cyber defence, rising applications, hardware, and networking and storage complexities?

8. CONCLUSION :

As technology tends to grow, the world is increasingly becoming a global village with almost all operating on the virtual worlds influencing most aspects of human life, enabling development, removing barriers to trade and allowing people across the globe to connect, collaborate and share ideas. Yet by the day hackers become more advanced. This puts the responsibility on the IT Experts to secure the IT infrastructure and users, hence necessity to be attentive and efficient in reacting to cyber attacks as well as proactive in ensuring that cyber threats are mitigated against them in their entirety. Cyber crime is increasing, and as such, cyber security needs to grow even faster if we hope to keep users online and, on the system, safe. The main aim of cyber security is the protection of harmful cyber-crime networks, applications and users over the internet.

Awareness of information security is crucial to rising cybercrimes and encouraging cyber protection. Currently there are so many uses of techniques, methods and tools to detect intrusion in the computer network and ongoing research is being done to make them even better to recognize intrusion. Yet new threats have emerged concurrently which will be hard for Handel as they want to change their behaviour. Within this paper we explained various techniques of machine learning applied to detect intrusions. Through the study, we argue that the approaches to machine learning are fit to identify anomalies through proper training, but the performance may vary according to different algorithms. Machine learning algorithms should also be applied in a manner that is sufficient to improve detection accuracy.

REFERENCES:

[1] Verma, P., Makwana, A. & Khan, S. (2015). Cyber Security: a Survey on Issues and Solutions. *International Journal of Advanced Research in Engineering and Technology*, *6*(4), 976–6480.

[2] Buczak, Anna L. Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, *18*(2), 11543–1176. https://doi.org/10.1007/BF01018580

[3] Hoque, Sazzadul Mukit, A. Naser, A. (2012). An Implementation of Intrusion Detection System Using Genetic Algorithm. *International Journal of Network Security & Its Applications*, *4*(2), 109–

120. https://doi.org/10.5121/ijnsa.2012.4208

[4] Roopak, M., Yun Tian, G. & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 452–457. https://doi.org/10.1109/CCWC.2019.8666588

[5] Neethu, B. (2014). Classification of Intrusion Detection Dataset using machine learning Approaches. *International Journal of Electronics and Computer Science Engineering*, *34*(3), 1044–1051. https://doi.org/10.3969/j.issn.0253-2417.2014.03.013

[6] Seissa, I. G., Ibrahim, J. & Yahaya, N. (2017). Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review. *International Journal of Science and Research (IJSR)*, *6*(1), 180–186. https://doi.org/10.21275/art20163936

[7] Duic, I., Cvrtila, V., & Ivanjko, T. (2017). International cyber security challenges. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 1309–1313. https://doi.org/DOI:10.23919/MIPRO.2017.7973625

[8] Durand, H. & Wegener, M. (2020). Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods. *Mathematics*, *8*(4). https://doi.org/10.3390/math8040499

[9] Wu, M., Song, Z. & Moon, Y. B. (2017). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-017-1315-5

[10] Nguyen, H. T. & Franke, K. (2012). Adaptive Intrusion Detection System via online machine learning. *12th International Conference on Hybrid Intelligent Systems, HIS*, 271–277. https://doi.org/10.1109/HIS.2012.6421346

[11] Zamani, Mahdi Movahedi, M. (2015). Machine Learning Techniques for Intrusion Detection. *ArXiv*. https://doi.org/10.4018/978-1-7998-2242-4.ch003

[12] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, *41*(4 PART 2), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

[13] Borkar, A., Donode, A., & Kumari, A. (2018). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). *Proceedings of the International Conference on Inventive Computing and Informatics, ICICI 2017, Icici*, 949–953. https://doi.org/10.1109/ICICI.2017.8365277

[14] Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H., Marufuzzaman, M., & Bian, L. (2017). Botnet detection using graph-based feature clustering. *Journal of Big Data*, *4*(1). https://doi.org/10.1186/s40537-017-0074-7

[15] Kozik, R., Choraś, M., Renk, R., & Hołubowicz, W. (2014). A Proposal of Algorithm for Web Applications Cyber Attack Detection. *IFIP International Conference on Computer Information Systems and Industrial Management*, *8838*. https://doi.org/10.1007/978-3-662-45237-0_61

[16] Wang, J., & Paschalidis, I. C. (2017). Botnet Detection Based on Anomaly and Community Detection. *IEEE Transactions on Control of Network Systems*, *4*(2), 392–404. https://doi.org/10.1109/TCNS.2016.2532804

[17] Wijesinghe, U., Tupakula, U., & Varadharajan, V. (2015). An enhanced model for network flow based botnet detection. *Conferences in Research and Practice in Information Technology Series*, *159*(January), 101–110.

[18] Haddadi, Fariba Cong, D. Le. (2015). On the Effectiveness of Different Botnet Detection Approaches. *Lecture Notes in Computer Science*, *9065*, 421–436. https://doi.org/10.1007/978-3-319-17533-1

[19] Akin, G., Bük, O., & Uçar, E. (2020). An inter-domain attack mitigating solution. *Turkish Journal of Electrical Engineering and Computer Sciences*, *28*(2), 757–772. https://doi.org/10.3906/elk-1904-179

[20] Zhang, Ningxia Yuan, Y. (2012). Phishing Detection Using Neural Network. *CS229*. https://doi.org/10.19026/rjit.6.2164

[21] Kato, K. & Klyuev, V. (2014). An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine. *International Journal of Intelligent Computing Research*, *5*(3), 464–471. https://doi.org/10.20533/ijicr.2042.4655.2014.0060

[22] Islam, R., & Abawajy, J. (2013). A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications*, *36*(1), 324–335. https://doi.org/10.1016/j.jnca.2012.05.009

[23] Smadi, S., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2015, December). Detection of phishing emails using data mining algorithms. In *2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (pp. 1-8). IEEE.

[24] Zahid, M., Inayat, I., Daneva, M. & Mehmood, Z. (2020). A security risk mitigation framework for cyber physical systems. *Journal of Software: Evolution and Process*, *32*(2), 1–15. https://doi.org/10.1002/smr.2219

[25] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, *37*(12), 7913–7921. https://doi.org/10.1016/j.eswa.2010.04.044

[26] Axelsson, S. (2015). *Intrusion Detection Systems : A Survey and Taxonomy Intrusion Detection Systems : A Survey and Taxonomy*. *April 2000*, 1–6. https://doi.org/10.20944/preprints202006.0065.v1

[27] Ibor, A. E., Oladeji, F. A. & Okunoye, O. B. (2018). A Survey of Cyber Security Approaches for Attack Detection, Prediction, and Prevention. *International Journal of Security and Its Applications*, *12*(4), 15–28. https://doi.org/10.14257/ijsia.2018.12.4.02

[28] Aissa, N. B. & Guerroumi, M. (2016). Semi-supervised Statistical Approach for Network Anomaly Detection. *Procedia Computer Science*, *83*(Fams), 1090–1095. https://doi.org/10.1016/j.procs.2016.04.228

[29] Azab, A., Alazab, M., & Aiash, M. (2016). Machine learning based botnet identification traffic. *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 1788–1794. https://doi.org/10.1109/TrustCom.2016.0275

[30] Huseynov, K., Kim, K. & Yoo, P. D. (2014, January). Semi-supervised botnet detection using ant colony clustering. In *Symp. Cryptography and Information Security (SCIS), Kagoshima, Japan*.

[31] Lin, W. C., Ke, S. W. & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*(1), 13–21. https://doi.org/10.1016/j.knosys.2015.01.009

[32] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2017). Feasibility of Supervised Machine Learning for Cloud Security. *ICISS 2016 - 2016 International Conference on Information Science and Security*, 31–35. https://doi.org/10.1109/ICISSEC.2016.7885853

[33] Shapoorifard, H., & Shamsinejad, P. (2017). A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques. *International Journal of Computer Applications*, *166*(3), 13–16. https://doi.org/10.5120/ijca2017913948

[34] Song, J., Takakura, H., Okabe, Y. & Nakao, K. (2013). Toward a more practical unsupervised anomaly detection system. *Information Sciences*, *231*, 4–14. https://doi.org/10.1016/j.ins.2011.08.011

[35] Zarca, A. M., Bernabe, J. B., Skarmeta, A., & Calero, J. M. A. (2020). *Virtual IoT HoneyNets to mitigate cyberattacks in SDN / NFV-enabled IoT networks*. *8716*(c), 1–15. https://doi.org/10.1109/JSAC.2020.2986621

[36] Ravikumar, G., & Govindarasu, M. (2020). Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning. *IEEE Transactions on Smart Grid*, *3053*(c), 1–1. https://doi.org/10.1109/tsg.2020.2995313

[37] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H. & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484–497.https://doi.org/10.1016/j.ins.2016.04.019

[38] Han, Y., Alpcan, T., Chan, J., Leckie, C., & Rubinstein, B. I. P. (2016). A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Transactions on Information Forensics and Security*, *11*(3), 556–570. https://doi.org/10.1109/TIFS.2015.2505680

[39] Xie, M., Hu, J. & Slay, J. (2014). Evaluating Host-based Anomaly Detection Systems : Application of the One-class SVM Algorithm to. *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 978–982. https://doi.org/10.1109/FSKD.2014.6980972

[40] Alsheikh, M. A., Lin, S., Niyato, D. & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys and Tutorials*, *16*(4), 1996–2018. https://doi.org/10.1109/COMST.2014.2320099

[41] Xu, X., Zuo, L. & Huang, Z. (2014). Reinforcement learning algorithms with function approximation: Recent advances and applications. *Information Sciences*, *261*, 1–31. https://doi.org/10.1016/j.ins.2013.08.037

[42] Shamshirband, S., Patel, A., Badrul, N. & Mat, L. (2014). Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. *Engineering Applications of Artificial Intelligence*, *2008*, 1–14. https://doi.org/10.1016/j.engappai.2014.02.001

[43] Xia, Z., Lu, S. & Li, J. (2010). *Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic A brief review of self-similarity*. *34*, 497–507.

[44] Rastegari, S., Hingston, P. & Lam, C. P. (2015). Evolving statistical rulesets for network intrusion detection. *Applied Soft Computing Journal*, *33*, 348–359. https://doi.org/10.1016/j.asoc.2015.04.041

[45] Huang, L. & Zhu, Q. (2019). Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. *Performance Evaluation Review*, *46*(2), 52–56. https://doi.org/10.1145/3305218.3305239

[46] Islam, S. N., Mahmud, M. A. & Oo, A. M. T. (2018). *Impact of optimal false data injection attacks on local energy trading in a residential microgrid*. *4*(1), 30–34. https://doi.org/10.1016/j.icte.2018.01.015

[47] Zimba, A., Wang, Z. & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

[48] Narang, P., Ray, S., Hota, C. & Venkatakrishnan, V. (2014). PeerShark: Detecting peer-to-peer botnets by tracking conversations. *Proceedings - IEEE Symposium on Security and Privacy*, *2014-Janua*, 108–115. https://doi.org/10.1109/SPW.2014.25

[49] Barraclough, P. A., Hossain, M. A., Tahir, M. A., Sexton, G. & Aslam, N. (2013). Intelligent phishing detection and protection scheme for online transactions. *Expert Systems with Applications*, *40*(11), 4697–4706. https://doi.org/10.1016/j.eswa.2013.02.009

[50] Coskun, B., Dietrich, S., & Memon, N. (2010). Friends of an enemy: Identifying local members of

peer-to-peer botnets using mutual contacts. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 131–140. https://doi.org/10.1145/1920261.1920283

[51] Wang, P., Sparks, S., & Cou, C. (2010). An advanced hybrid peerto- peer botnet. *IEEE Transactions on Dependable and Secure Computing*, *7*(2), 113–127. https://doi.org/10.1109/TDSC.2008.35

[52] Wu, S. X., & Banzhaf, W. (2010). *The use of computational intelligence in intrusion detection systems : A review*. *10*, 1–35. https://doi.org/10.1016/j.asoc.2009.06.019

[53] Nappa, A., Fattori, A., Balduzzi, M., Dell'Amico, M., & Cavallaro, L. (2010). Take a deep breath: A stealthy, resilient and cost-effective botnet using skype. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6201 LNCS*, 81–100. https://doi.org/10.1007/978-3-642-14215-4_5

[54] Zhong, R., & Yue, G. (2010). DDoS Detection System Based on Data Mining. *Proceedings of the Second International Symposium on Networking and Network Security*, *1*, 062–065. http://academypublisher.com/proc/isnns10/papers/isnns10p62.pdf

[55] Nguyen, H. V., & Choi, Y. (2010). Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDos framework. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *4*(3), 640–645. https://doi.org/10.5281/zenodo.1072908

[56] Xiang, Y., Li, K., & Zhou, W. (2011). *Low-Rate DDoS Attacks Detection and Traceback by*. *6*(2), 426–437.

[57] Fedynyshyn, G., Chuah, M. C. & Tan, G. (2011). Detection and classification of different botnet C&C channels. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6906 LNCS*, 228–242. https://doi.org/10.1007/978-3-642-23496-5_17

[58] Saad, Sherif traore, Issa ghorbani, Ali. (2011). Detecting P2P Botnets through Network Behavior Analysis and Machine Learning. *Ninth Annual International Conference on Privacy, Security and Trust Detecting*. https://doi.org/10.1109/PST.2011.5971980

[59] Zhang junjie, Perdisci Roberto, Lee Wenke, X. L. and S. U. (2011). Detecting Stealthy P2P Botnets Using Statistical Traffic Fingerprints'.pdf. *2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*. https://doi.org/10.1109/DSN.2011.5958212

[60] Wu, Y. (2011). *DDoS detection and traceback with decision tree and grey relational analysis Huei-Ru Tseng Wuu Yang * and Rong-Hong Jan*. *7*(2), 121-136.

[61] Raj Kumar, P. A. & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, *34*(11), 1328–1341. https://doi.org/10.1016/j.comcom.2011.01.012

[62] Karimazad, R. & Faraahi, A. (2011). An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks. *2011 International Conference on Network and Electronics Engineering*, *11*, 44–48.

[63] Udhayan, J. & Hamsapriya, T. (2011). Statistical segregation method to minimize the false detections during DDoS attacks. *International Journal of Network Security*, *13*(3), 152–160.

[64] Sa, M. & Rath, A. K. (2011). A Simple Agent Based Model for Detecting Abnormal Event Patterns in a Distributed Wireless Sensor Networks. *International Journal of Computer Science and Security, (IJCSS)*, *4*(6), 580-588.

[65] Zang, X., Tangpong, A., Kesidis, G. & Miller, D. J. (2011). Botnet Detection Through Fine Flow Classification. *Science*, *0915552*, 1–17.

[66] Gupta, B. B., Joshi, R. C. & Misra, M. (2012). ANN based scheme to predict number of zombies in a DDoS attack. *International Journal of Network Security*, *14*(2), 61–70.

[67] Garasia, S. S., Rana, D. P. & Mehta, R. G. (2012). HTTP botnet detection using frequent patternset

mining. *International Journal of Engineering Science & Advanced Technology,* 2(3), 619-624.

[68] Jeyanthi, N. & Sriman Narayana Iyengar, N. C. (2012). An entropy based approach to detect and distinguish DDoS attacks from flash Crowds in VoIP Networks. *International Journal of Network Security*, *14*(5), 257–269.

[69] François, J., Aib, I. & Boutaba, R. (2012). FireCol: A collaborative protection network for the detection of flooding DDoS attacks. *IEEE/ACM Transactions on Networking*, *20*(6), 1828–1841. https://doi.org/10.1109/TNET.2012.2194508

[70] Warriach, E. U. (2013). *Fault Detection in Wireless Sensor Networks : A Machine Learning Approach*. https://doi.org/10.1109/CSE.2013.116

[71] Lee, S. & Kim, J. (2013). Fluxing botnet command and control channels with URL shortening services. *Computer Communications*, *36*(3), 320–332. https://doi.org/10.1016/j.comcom.2012.10.003

[72] Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A. & Garant, D. (2013). Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security*, 1–15. https://doi.org/10.1016/j.cose.2013.04.007

[73] Sharma, A. K. & Parihar, P. S. (2013). An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *2*(7), 249–256.

[74] Louvieris, P., Clewley, N. & Liu, X. (2013). Effects-based feature identification for network intrusion detection. *Neurocomputing*, *121*, 265–273. https://doi.org/10.1016/j.neucom.2013.04.038

[75] Kaur, Gursheen Singh, M. (2014). Detection of Black Hole in Wireless Sensor Network based on Data Mining. *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, *2014*, 457461. https://doi.org/10.1017/CBO9781139058452.002

[76] Stevanovic, M. & Pedersen, J. M. (2014). An efficient flow-based botnet detection using supervised machine learning. *2014 International Conference on Computing, Networking and Communications, ICNC 2014*, 797–801. https://doi.org/10.1109/ICCNC.2014.6785439

[77] Rao, R. S. & Ali, S. T. (2015). A computer vision technique to detect phishing attacks. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 596–601. https://doi.org/10.1109/CSNT.2015.68

[78] Bhuyan, M. H., Bhattacharyya, D. K. & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, *51*, 1–7. https://doi.org/10.1016/j.patrec.2014.07.019

[79] Hoque, N., Bhattacharyya, D. K. & Kalita, J. K. (2016). A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. *2016 8th International Conference on Communication Systems and Networks, COMSNETS 2016*, *1*, 1–2. https://doi.org/10.1109/COMSNETS.2016.7439939

[80] He, Z., Zhang, T. & Lee, R. B. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 114–120. https://doi.org/10.1109/CSCloud.2017.58

[81] Alejandre, F. V., Cortés, N. C., & Anaya, E. A. (2017). Feature selection to detect botnets using machine learning algorithms. *2017 International Conference on Electronics, Communications and Computers, CONIELECOMP 2017*. https://doi.org/10.1109/CONIELECOMP.2017.7891834

[82] Kim, J. & Park, J. (2018). FPGA-based network intrusion detection for IEC 61850-based industrial network. *ICT Express*, *4*(1), 1–5. https://doi.org/10.1016/j.icte.2018.01.002

[83] Ilavendhan, A. & Saruladha, K. (2018). Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express*, *4*(1), 46–50. https://doi.org/10.1016/j.icte.2017.12.002

[84] Ferreira, M. (2019). Malicious URL detection using machine learning algorithms. In *Proc. Digit. Privacy Security Conf.* (pp. 114-122).

****