ISSN: 0974-6471, Vol. 13, No. (1) 2020, Pg. 01-21

Oriental Journal of Computer Science and Technology

www.computerscijournal.org

Performance of Machine Learning and other Artificial Intelligence Paradigms In Cybersecurity

GABRIEL KABANDA

Atlantic International University, 900 Fort Street Mall 40, Honolulu, Hawaii 96813, USA.

Abstract

Cybersecurity systems are required at the application, network, host, and data levels. The research is purposed to evaluate Artificial Intelligence paradigms for use in network detection and prevention systems. This is purposed to develop a Cybersecurity system that uses artificial intelligence paradigms and can handle a high degree of complexity. The Pragmatism paradigm is elaborately associated with the Mixed Method Research (MMR), and is the research philosophy used in this research. Pragmatism recognizes the full rationale of the congruence between knowledge and action. The Pragmatic paradigm advocates a relational epistemology, a non-singular reality ontology, a mixed methods methodology, and a value-laden axiology. A qualitative approach where Focus Group discussions were held was used. The Artificial Intelligence paradigms evaluated include machine learning methods, autonomous robotic vehicle, artificial neural networks, and fuzzy logic. A discussion was held on the performance of Support Vector Machines, Artificial Neural Network, K-Nearest Neighbour, Naive-Bayes and Decision Tree Algorithms.

Article History

Received: 02 April 2020
Accepted: 19 May 2020

Keywords

Artificial Intelligence;
Artificial Neural Networks;
Bayesian Network;
Cybersecurity;
Deep Learning;
Machine Learning.

Introduction

Background

Cyber security is the collection of policies, techniques, technologies, and processes that work together to protect the confifidentiality, integrity, and availability of computing resources, networks, software programs, and data from attack (Berman, D.S., *et al.,* 2019). The process of instructing computers to learn is called machine learning. Machine learning (ML) algorithms inspired by the central nervous system are referred to as Artifificial neural networks (ANNs), and this involves programming computers to teach themselves from data instead of instructing them to perform specific tasks. Deep Learning (DL) is a special category of ML purposed to bring it to closer to Artificial Intelligence (AI). ML is known for automating the analysis of large data sets and producing models of the general relationships found among the data.

CONTACT Gabriel Kabanda gabrielkabanda@gmail.com Atlantic International University, 900 Fort Street Mall 40, Honolulu, Hawaii 96813, USA.

Doi: 10.13005/ojcst13.01.01

According to Truong, T.C., *et al.,* (2020), the three classes of ML are as follows as illustrated on Figure 1 below:

- Supervised learning: where training examples are given to the methods in the form of inputs labeled with corresponding outputs;
- Unsupervised learning: where unlabeled inputs are given to the methods;
- Reinforcement learning: where data used is in the the form of sequences of actions, observations, and rewards.

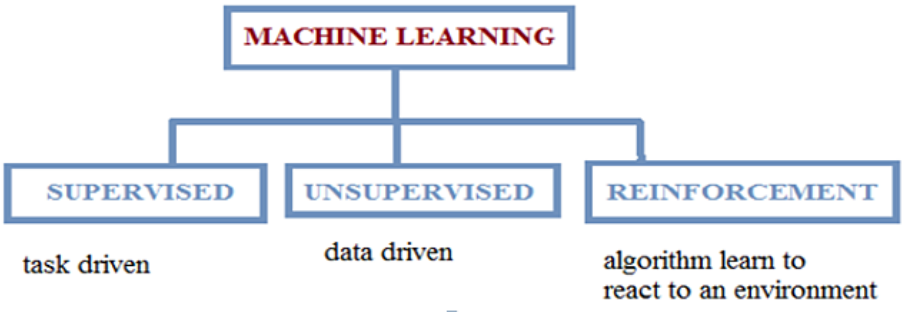


Fig. 1: Three levels of Machine Learning
(Source: Proko, E., Hyso, A., and Gjylapi, D. (2018). Machine Learning Algorithms in Cybersecurity, http://www.CEURS-WS.org/Vol-2280/paper-32.pdf)

The research is purposed to evaluate the performance of Machine Learning and other Artificial Intellligence paradigms use in Cybsersecurity. The phenomenal growth in the use of the internet and its associated threats have precipitated the Network Intrusion Detection Systems (NIDS). The NIDS is a category of computer software that monitors system behaviour with a view to ascertain anomalous violation of security policies and distinguishes between the legitimate network users from malicious ones (Bringas, P.B., and Santos, I., 2010, p.229).

NIDS exist in two categories, anomaly detectors and misuse network detectors. Misuse detection systems invigilate all incoming traffic to detect any sequence that appears in that knowledge base. On the contrary, anomaly detection systems focus on discovering new unknown threats (Bringas, P.B., and Santos, I., 2010, p.229). Research conducted by Bringas and Santos (2010, p.229) on Artificial Intelligence paradigms for use in network anaomaly detection focused on neural networks, genetic algorithms, fuzzy logic, support-vector machines, finite automata, and other diverse data-mining-based approaches.

Information Systems Security (ISS) comprises computer security and communications security. The normal requirement for network security is an Intrusion Detection Systems(IDS) and Intrusion Prevention Systems (IPS). A firewall provides network security against external threats in order to preserve sensitive files on computers within the network (Stallings, W., 2015, p.10). Each of the devices on the network can be thought of as a node; each node has a unique address. The phenomenal growth of the use of wireless technology has increased the vulnerability of networks (Stefanova, Z.S., 2018, p.2). Consequently, the use of a firewall as one of the classical security measures has proved to be inadequate. The cyber-criminals have now become innovative with their new techniques.

Cybersecurity is purposed to protect internet-connected systems from cyberattacks. Gercke (2012) defined cybercrime as a computer related crime, and Oxford English Dictionary (2019) defined it as criminal activities carried out by means of computers or the internet. Governments, companies, organisation and individuals throughout the world are struggling to deal with cybercrimes, and the most forms of cyberattacks are ransomware, email phishing, cyber bullying, online extortions, etc (Yedaly, M., and Wright, B., 2016; Norton Symantec, 2017). Cybersecurity culture is defined as the beliefs, assumptions, attitudes, values, perceptions and knowledge that people have pertaining to

cybersecurity and how these manifest in their interaction with ICTs (European Union Agency for Network and Information Security, 2017). Technology alone cannot be a cushion against cyber- threats, but instead humans should occupy a centre stage through cyber security culture (Gcaza *et al.,* 2017). A strong cybersecurity culture changes the mindsets of people and their security behaviour (European Union Agency for Network and Information Security, 2017) and will stand as a human firewall against threats without coercion. The emergence of information and communication technologies (ICTs) has precipitated a dependent information society supportive of business management, information sharing and provision of electronic services (Malyuk and Miloslavskaya, 2016). In Africa, most organizations are not ready to respond to information security threats (Africa Cyber Security Report, 2016). These range from online visa applications to e-government platforms and this has made them prime targets for cyber-attacks (Africa Cyber Security Report, 2017). New technologies and business process automation is being done without ensuring that adequate security controls are put in place to safeguard these systems (Africa Cyber Security Report, 2016). There is a dire need to nurture an information society that exhibits a culture of respecting values, rights and freedoms in terms of accessing information so as to build confidence and trust in the use of ICTs in Africa (United Nations, 2014). In Africa, twenty-one countries have Data Protection Legislations and 13 have both Data and Cyber Security Legislation.

The overall security in Cybersecurity is only as strong as the weakest link (Nielsen, R., 2015, p.8). It is of primordial importance that the company objectives clearly reflect access controls and security mechanisms. Common practice shows that employees are given access to only what they need, the internet is segregated into separate networks that compartmentalize security and access privileges are limited to minimise any security breaches (Nielsen, R., 2015, p.11). Nielsen (2015, p.12) argues that Virtual Private Networks or VPNs are known to provide secure access to internal company internet by employees on the Internet working from elsewhere outside the company premises. The recommended network structure that provides a secure internet environment is shown on Figure 2 below (Neilsen, R., 2015, p.14).

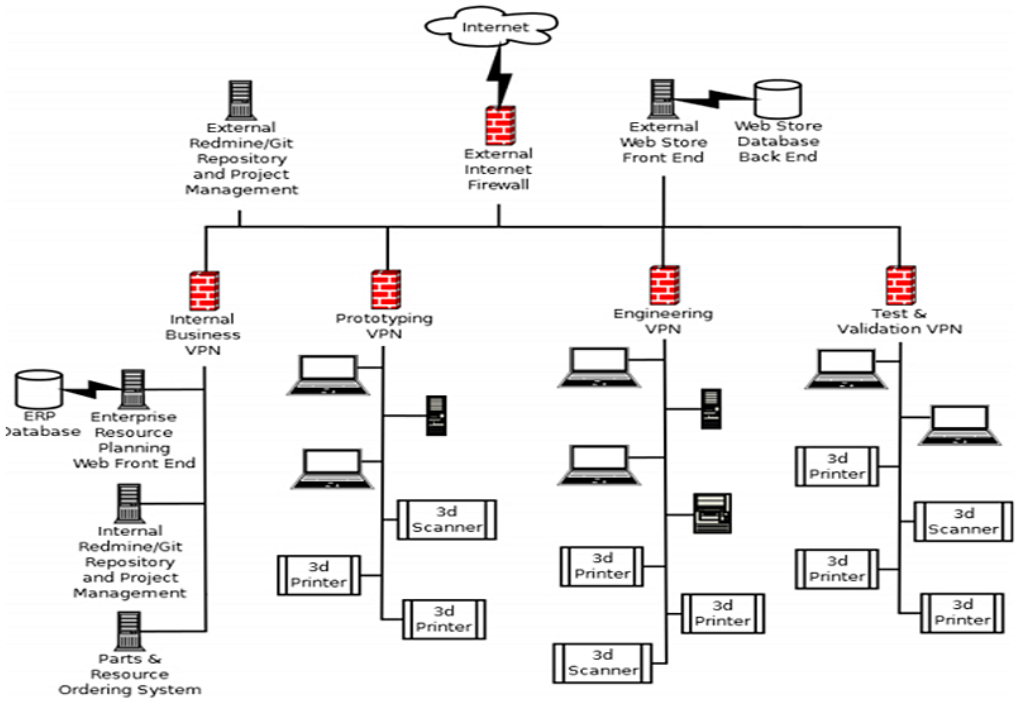


Fig. 2: Recommended Network Structure (Source: Nielsen, R., 2015, p.14)

Convergence of wired and wireless services is dependent upon the progress made by the next-generation access networks. The broad-band evolution coupled with the phenomenal growth in the Internet has precipitated intense traffic patterns in access networks (Yu, J., *et al.,* 2009, p.1). A unified networking platform for fixed and mobile users is now clothed with mobility features that deliver voice, data, and video services (Yu, J., *et al.,* 2009, p.1).

The first step in Network Security is to redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. This can be strengthened by providing VPN support (Nielsen, R., 2015, p.18). Separation of duties is one of the key principles of information security which can be supported by authentication and authorization systems that give access only to those business resources needed to perform one's duties. As shown on Figure 1, this separation can be achieved through VPNs. A VPN provides mobility to the users to work on-site or off-site. However, in this separation of duties, there is need for an Intrusion Detection Systems(IDS) and Intrusion Prevention Systems (IPS) that prevents the detected attack from taking place and to protect the network (Nielsen, R., 2015, p.19). The IDS often operates with sensors, analyzers and a user interface, as shown Figure 3 below. A firewall provides network security against external threats (Stallings, W., 2015, p.10). Operating Systems Hardening is one of the basic steps to secure an operating system (Stallings, W., 2015, p.28). This involves installing and patching the operation system, and then hardening and/or configuring the operating system to adequately provide acceptable security measures.

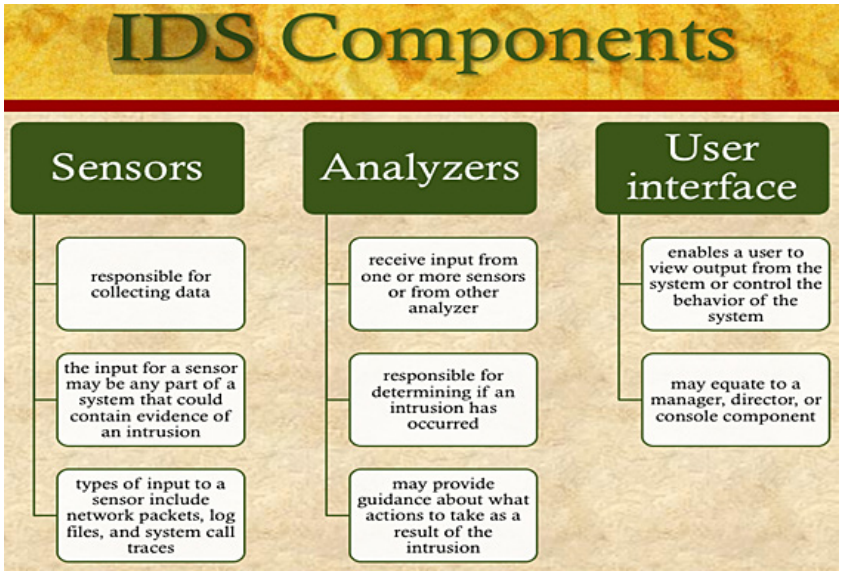


Fig. 3: The IDS Components (Source: Stallings, W., 2015, p.6)

The phenomenal increase in internet-connected systems has precipiated an increase in the attack surface which has led to greater risk of cyber attack (Berman, D.S., *et al.,* 2019). The cyber attacks are increasigly getting sophisticated with zero-day exploits and malware that evade security measures. Furthermore, commercial interest in cyber attacks has increased. We may need to leverage data analytics in cyber defense systems. Truong, T.C. (2020) observed that cybersecurity systems are increasingly getting used to improve operational efficiencies and reduce costs in critical areas, such as finance, transportation, defence, healthcare.

Statement of the Problem

The phenomenal growth in the use of the internet and its associated threats have precipitated the

Network Intrusion Detection Systems (NIDS). The rapid growth of the use of wireless technology has increased the vulnerability of networks. Classical security measures have proved to be grossly inadequate under the circumstances. The focus for Cybersecurity has now shifted to the use of Artificial Intelligence paradigms for use in network anomaly detection such as neural networks, genetic algorithms, fuzzy logic, support-vector machines, finite automata, and other diverse data-mining-based approaches. The key problem is to evaluate various Artificial Intelligence paradigms for use in Cybersecurity in support of Bayesian Networks.

Purpose of Study

The research is purposed to evaluate machine learning and other artificial intelligence algorithms for use in Cybersecurity.

Research Objectives

The research objectives are to:

Which artificial intelligence paradigm is most effective in developing a Cybersecurity system than can handle a higher degree of complexity?

The sub questions are:

- How are the Artificial Intelligence paradigms for use in network detection and prevention systems ?
- How is a Cybersecurity system developed that uses artificial intelligence paradigms and can handle a high degree of complexity?

Literature Review

Overview

Each of the devices on the network can be thought of as a node; each node has a unique address. The first step in Network Security is to redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. Intrusion detection and prevention systems (IDPS) include all protective actions or identification of possible incidents, analysing log information of such incidents, how to block them in the beginning itself and generate reports for the concern of security personnel (Umamaheswari, K., and Sujatha, S., 2017, p.1). Stallings (2015, p.31-38) recommends the use of various security control measures in an organisation.

Table 1: Anomaly detection methods (Source: Karimpour *et al.,* (2016, p.3)

Method	Data type	Attack	Proposed system	Accuracy
Graph in time series	Flow-based	DDoS	Graph-based	94.2%
Dispersion graph	Flow-based	DDoS	Graph-based	100%
Using flow concept	Flow-based	Dictionary	Flow-based	99%
Graph clustering and local deviation coefficient	Packet-based	DoS, Scan	Graph-based	95.3%
Graph clustering and local deviation factor	Packet-based	DoS, Scan	Graph-based	97.2%
Packet heard analyzing	Packet-based	DoS, Scan	Packet-based	95.4%

Table 2: Various attack descriptions (Source: Karimpour *et al.,* 2016, p.4)

Attack type	Description
DoS	Denial of service; an attempt to make a network resource unavailable to its intended users: temporarily interrupt services of a host connected to the Internet
Scan	A process that sends client requests to a range of server port addresses on a host to find an active port
Local access	The attacker has an account on the system in question and can use that account to attempt unauthorized tasks
User to root	Attackers access a user account on the system and are able to exploit some vulnerability to gain root access to the system
Data	Attackers involve someone performing an action that they may be able to do on a given computer system, but that they are not allowed to do according to policy

Network attack detection is derived from network detection systems. From an analysis of packet contents of the network, one can find the attacks or malicious behavior. A general view of these intrusion detection methods are shown on Table 1 below.

The outcome of the research by Karimpour *et al .,* (2016, p.4) showed various attack descriptions shown on Table 2.

$$AveW = [\Sigma^{N}_{i=1} (Wi) - (\Sigma^{N}_{i=1} ExtW_{i}) / N]/N$$

The research article by Demir and Dalkilic (2017) came out with a threat model which assumed that there is a monitoring system that collects information on the packet level. However, these assumptions may not always hold water. According to Umamaheswari and Sujatha (2017), the components in IDPSs can be sensors or agents, management and database servers, user and administrator consoles for interaction and management networks. There is need for protection of the software-based IDPS components such that their operating systems and applications are kept fully up-to-date. Umamaheswari and Sujatha (2017) proposed a model of defence framework which arranges intrusion detection components in a maze-like structure so as to capture and dynamically correlate unknown attacks as early as possible.

According to Williams (2014), cyberspace is a human made information environment created when computers and related telecommunication equipment and other components that allow fast movement of large amounts of data are connected. The use of IP addresses exposes the nonphysical nature of cyberspace. In the physical domain, addresses reference a physical location but IP addresses tell the user where to go, without necessarily pointing to a physical location. All the interconnected devices and data that comprise cyberspace are manmade. Cyberspace is categorized into three layers namely the physical layer, the logical layer and the social layer.

The Internet of Things (IoT) relates to interconnected devices via communication channels and methods that transmit and communicate with each other. The transmission method can be wired or wireless depending on the devices. According to Symantec (2016), the Internet of Things is now a prime target for hackers. Risks include data falsification, data manipulation, data and identity theft or IP theft. The number of Internet of Things (IoT) devices is increasing and those devices are being used every day (Concierge Security report, 2018).The Internet of Things (IoT) industry is expected to be worth $US19 trillion by 2020 globally (ACS, 2016). Furthermore, the growth in big data and cloud computing industries also present great chances for the Internet of Things (IoT) industry to flourish. However, cybersecurity is a key challenge in the Internet of Things (IoT) realm. This is because hackers can penetrate an organization's network through the Internet of Things (IoT) devices (MacAfee, 2018) or through the cloud environment which the Internet of Things (IoT) devices heavily rely on (KPMG, 2018).The security of those devices together with the people that use them is very important as cybersecurity risk is high (Concierge Security report, 2018).

According to Fehling *et al.,* (2014), the cloud symbol is usually used to symbolize the internet. Cloud computing is now frequently used to describe the delivery of software, middleware platforms, infrastructure, whole business processes and storage services over the internet. These services are delivered when they are needed in the quantity needed at a certain time. Put differently, cloud computing is very much similar to the rent-a-car model. The cost effectiveness and efficiency of the cloud platforms is tempting most organizations to migrate to the cloud and enjoy a wide range of benefits (Sharma, 2012) which according to KPMG (2018) include:

- free capital expenditure
- accessibility from anywhere at anytime
- no maintenance headaches
- improved control over documents as files will be centrally managed

The cloud computing market grew 4 times between 2015 and 2020 from US73 billion to US270 billion as depicted on Figure 4 above (KPMG, 2018). Cybersecurity is also a key challenge in this industry as cybercriminals use cloud services as warehouses to store their malicious software and as targets that will be used as launchpads for Denial of Service (DOS) attacks (MacAfee, 2018).

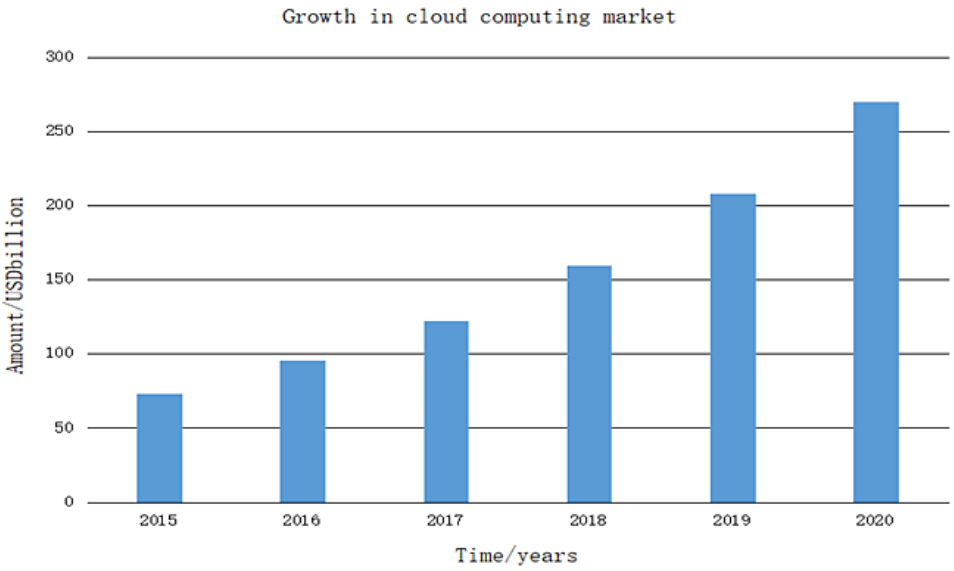


Fig.4: Projection of growth of the Cloud Computing market. Source: KPMG (2018)

Cybercrime has matured with a big market with several stakeholders and is unlikely to stop as it is very rewarding. Online criminal marketplaces have gone to the extent of selling ransomware services and products. End users of technology continue to fail to adhere to basic security norms and this sustains the cybercrime market (MacAfee, 2018). Cybercrime features on the top 10 global risks together with terrorist attacks, natural disasters and extreme weather patterns KPMG (2018). According to MacAfee (2014) and World Economic Forum (2017) as cited by KPMG (2018), cybercrime costs the world $US 575 billion annually which constitute 0.5% of the world's Gross Domestic Product. The damage caused by cybercrime is also expected to reach US$6 trillion by 2021 (KPMG, 2018). Cybercrime is expected to grow taking advantage of poor security of the Internet of Things (IoT) devices (MacAfee, 2018). Cybercriminals are also riding on Artificial Intelligence (AI) to make and replicate malicious software as well as identifying weak targets.

Table 3 below shows several forms of cybercrime and their associated estimated daily activity.

Ransomware erupted in 2015 and is likely to continue to be very popular going forward whilst improving in sophistication. It is anticipated that businesses are going to be facing ransomware attacks every 14 seconds by 2019 and the attacks on healthcare systems is expected to quadruple by 2020 (Concierge Security report, 2018).

Table 3: Table of cybercrimes and their estimated daily activity

Cybercrime	Estimated Daily Activity
Ransomware	4 000
Phishing	33 000
New malicious software/malware	300 000
Records lost to hacking	780 000
Malicious scans	80 billion

Source: MacAfee (2018)

Figure 5 below shows the difference between information security and cybersecurity. Information security culture consist of perceptions, attitudes, assumptions, values and knowledge that guide the interaction of people with organisational information assets with the mandate of securing information (Al Hogail, 2015). On the other hand cyber security culture is defined as the beliefs, assumptions,

attitudes, values, perceptions and knowledge that people have pertaining to cyber security and how these manifest in their interaction with Information Communication Technologies (European Union Agency for Network and Information Security, 2017).

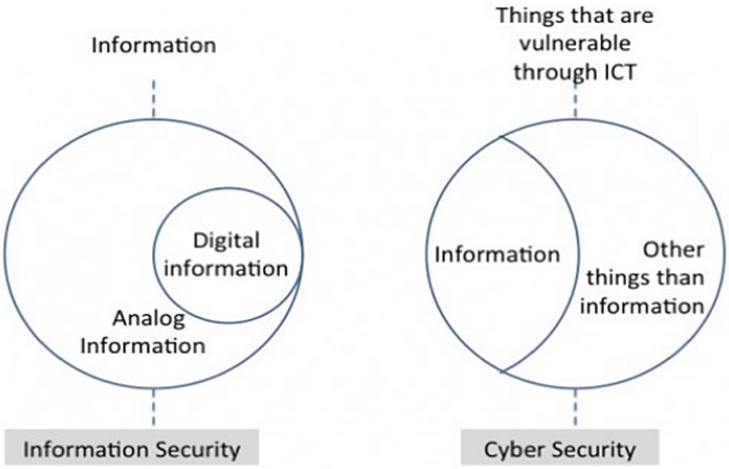


Fig.5: Differences between Information Security and Cybersecurity. Source: Center for Cyber and Information Security
(https://ccis.no/cyber-security-versus-information-security/)

The NIST Cybersecurity Framework

According to National Institute of Standards and Technology (2018), the NIST Cybersecurity framework was crafted with the view of reducing cyber risk and improve security to critical infrastructure. It is based on standards such as Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). This framework is not a one size fits all (Purdy, 2016) framework since different organizations face different cybersecurity risks. The framework targets companies, Non-Governmental Organizations, government agencies as well as communities regardless of their size and focus. The framework consists of three main components which include the framework core, implementation tiers and the framework profile.

Fig.6: NIST Cybersecurity Framework Core components. Source: National Institute of Standards and Technology (2018)

The NIST (2018) indicates that this component of the framework consists of five sub- components or activities which are to identify, protect, detect, respond and recover from cyber-attacks as shown below on Figure 6.

The framework core can also be viewed as a set of cybersecurity activities, desired outcomes and references applicable and common across all sectors. Each function has categories (total of 22) and subcategories (total of 98) (Angelini *et al.,*

2017). Subcategories are basically practical activities that have to be done such as data collection on the organization's software and hardware or even documenting legal requirements for cybersecurity (Angelini *et al.,* 2017). Informative references are the international standards that are associated with each category and subcategory. The implementation of all the subcategories by an organization will result in a high cybersecurity level. However, it is important to note that the cybersecurity framework was primarily designed for critical infrastructure although it can be used by smaller companies and communities. According to Alcaraz and Zeadally (2015), critical infrastructure is made up of assets and systems which can be either virtual or physical that are so important to a nation such that any interruption of their services could have a serious impact on economic well-being, national security, public health or safety or a combination of all of these. Critical infrastructure includes power grids, hospital systems as well as public transportation.

Machine Learning

Computers have always operated on commands with a set of known responses programmed into them, with no room for deviation. Technology has developed to allow computers to learn new responses based on data they receive. This helps them complete tasks that were not originally programmed into them as they interact with their users. This technology is called Machine Learning and forms part of artificial intelligence (AI). In Machine Learning (ML) we focus on the computer programs that have access to large volumes of data from which they can learn by themselves. There are unlimited opportunities in ML for detecting network intrusion without using a signature database.

The use of AI and ML in Cybersecurity realises benefits which include faster response and protection, automated protection, learning to adapt to various challenging situations, personalization, and usabaility. The major applications of ML are as follows:

Virtual Personal Assistants

Computing smart devices are equipped with voice recognition applications that respond to commands given by the user. In the beginning the responses are basic and at times have errors. However, over time as the application develops the user's patterns and preferences, the responses become more complex and accurate. Examples of such applications are Siri, Alexa, Google, etc., the more popular virtual personal assistants that can be asked to recommend a good restaurant in an area the user is visiting.

Predictions while Commuting

Utilising GPS navigation services, motorists can be advised by a machine learning computer of the least congested or shortest to a predetermined destination. Users seeking public transport, can book a taxi using an application of their device. This application will search for the closest available taxi and provide an estimated cost of the journey to the desired destination.

Videos Surveillance

Artificial intelligence is characterised by the ability to learn, comprehend and and predict human behaviour. This assists users to prevent possible mishaps in public areas.

Social Media Services

ML is now being utilized in targeting advertisements, personalization of news, and social media platforms. In this way, ML enables online connection with people whose learning profiles arae available on various platforms such as Facebook. Facial recognition can also help identify the established connection of people from pictures uploaded online.

Email Spam and Malware Filtering

ML can filter possible spam from email patterns of users and common recipients, machine learning can filter possible spam. Also, by learning certain code, it can detect different malware

Customer Support Services

To reduce the dependence on large number of call centre support agents, organisations are utilising chatbots that respond to basic customer queries. With time they are learning to respond to more complex questions as they continuously interact with the clients with better answers.

Search Engine Result Refining

The manner in which users respond to a set of search results provide machine learning with data to build a predictive pattern to improve future search

results. Google, Bing, etc., use such backend algorithms.

Product Recommendations
ML is useful in predicting and recommending the desired products to users on shopping websites.

Online Fraud Detection
Funds transfer patterns are learnt by ML through determination of genuine and potentially fraudulent online transactions.

Complexity of Cyber-Physical Systems
Cybercrimes are monotonically increasing and there is a growing concern on the security, confidentiality and computer assurance of the stored data. Intrusion detection and prevention systems (IDPS) include all protective actions or identification of possible incidents, analysing log information of such incidents, how to block them in the beginning itself and generate reports for the concern of security personnel (Umamaheswari, K., and Sujatha, S., 2017, p.1).

The complexity of cyber-physical systems (CPS), the roles and responsibilities of the humans that interact with them, and the cyber-security of these highly interconnected systems now requires a resilient CPS (Ghafouri, A., 2018, p.1). According to Ghafouri, resilient CPS provide interdisciplinary solutions for problems such as how to tailor the control system to enable it to respond to disturbances quickly and efficiently, how to better integrate widely distributed CPS to prevent faults that result in disruptions to operations of critical infrastructure, and how to design cyber-security protection mechanisms so that the system defends itself from cyber-attacks by changing its behaviors. Advanced control algorithms deployed in CPS are dependent upon data from multiple sensors to predict the behaviors of the system and make corrective responses. However, such systems can become brittle to the extent that any unrecognized fault or degradation in the sensors can lead to incorrect responses by the control algorithm and potentially compromise the desired operation. Ghafouri, A. (2018, p.1) argued that advanced control algorithms in resilient CPS require the implementation of detection and diagnosis architectures to recognize sensor faults and degradations.

A significant challenge is the design of anomaly detectors that effectively detect failures and cyber-attacks in CPS. In design and evaluation of anomaly detectors, realistic attack models that represent the harmful effects of cyber-attacks on CPS are needed (Ghafouri, A., 2018, p.2). Resilience in CPS is defined as protecting the operational goals (e.g., stability) as well as other non-operational goals (e.g., privacy) in the presence of both expected events (e.g., failures) and unexpected events (e.g., cyber-attacks) (Ghafouri, A., 2018, p.6). According to Ghafouri, A. (2018, p.6), resilience in CPS must attain three goals:

- Integrity which represents the trustworthiness of data or resources,
- Availability which is the ability to access and use information on demand as specified, and
- Confidentiality, which is the ability to keep information secret or private from unauthorized users.

Research Methodology
Presentation of the Methodology
The Pragmatism paradigm which is intricately related to the Mixed Methods Research (MMR) was used in this research. Pragmatism makes use of the rationale of the congruence between knowledge and action. The Mixed Methods approach consisted of a qualitative aspect whose research design was Focus Group discussions, and the quantitative aspect whose research design was an Experiment.

A research design symbolises advance planning or a research master plan (Kothari, C.R., 2004). This planning caters for the research methods to be used, techniques to analyse the data whilst addressing the objectives of the research and taking into account the resources available. Research design is required because it helps the smooth flow of the several research processes, thereby making research efficient in getting more information with less investment in time, effort and money (Kothari, C.R., 2004). The relationship between research methodology and research design are amply illustrated by the research onion shown on Figure 7 below.

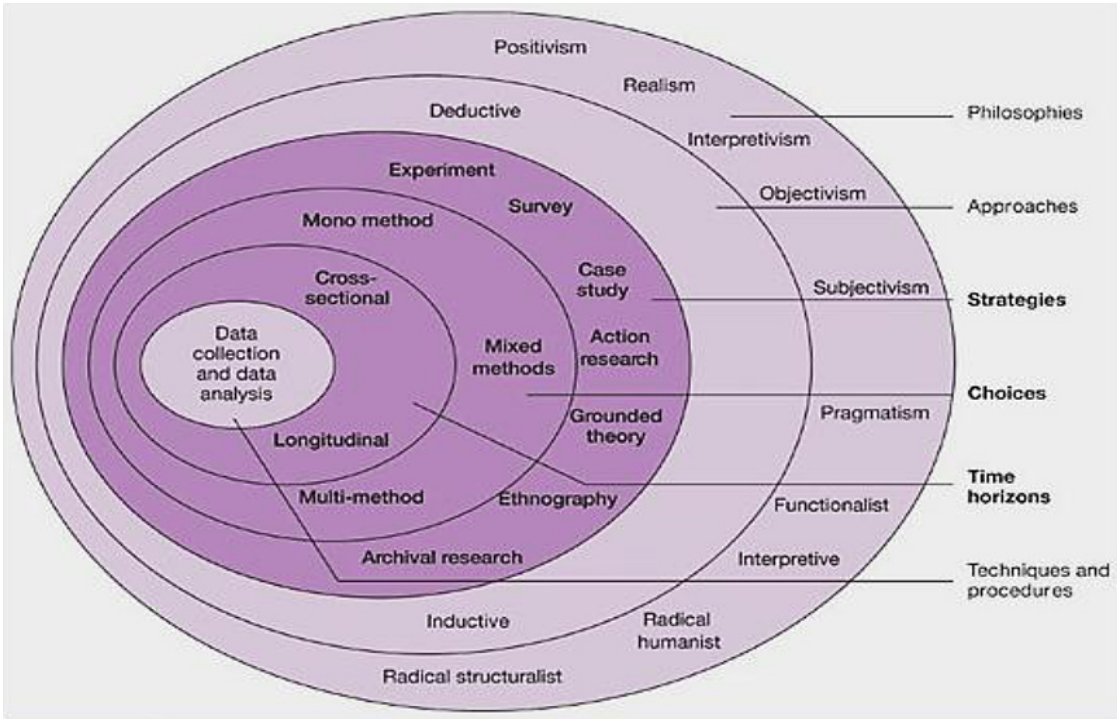


Fig.7: The Research Onion (Sources: Saunders *et al*., 2009, p.108).

With unsupervised classification, it is assumed that there is no external teacher that can train the classifier. The desirable position in cases of applications where the expected results are not known in advance is to train the classifier. In AI the algorithms can be improved by employing problem solving techniques used by human beings, such as learning, or gaining the ability to perform tasks from examples and training.

Qualitative data for this research was collected on the cybersecurity framework and industry practice. Focus Group discussions were held in order for the participants to interact and share their experiences whilst influencing one another's views and contributions. The researcher facilitated the Focus Group discussions on a Cybersecurity workshop with a total of 8 participants held at the Harare International Conference Centre (HICC), on Thursday 7th and Friday 8th March, 2019.

The first aim for analysis of qualitative data is to describe a phenomenon in some or greater detail. According to Flick, U. (2013, p.7), the first approach in the qualitative data analysis puts subjective experiences as the focus. A second approach focuses on describing the making of a social situation. A third approach is to go beyond the first two approaches and into spheres of implicit and even unconscious aspects of a social phenomenon.

For the research to be credible special attention has to be paid to reliability and validity. Reliability measures consistency of the instrument in measuring. To test for reliability of the instrument, the Cronbach's alpha coefficient was used to check for internal consistency. To be reliable the minimum threshold for the Cronbach's alpha coefficient is 0.7 (Saunders *et al.,*2009). Reliability tests were conducted for the observation data and the key variables chosen.

There are two types of validity which are internal and external validity. Internal validity consists of face validity and construct validity. According to Saunders *et al.,* (2009) reliability is the extent to which the techniques used for data collection and analysis could give the same results . It also concerns issues of whether same results would be found if the same

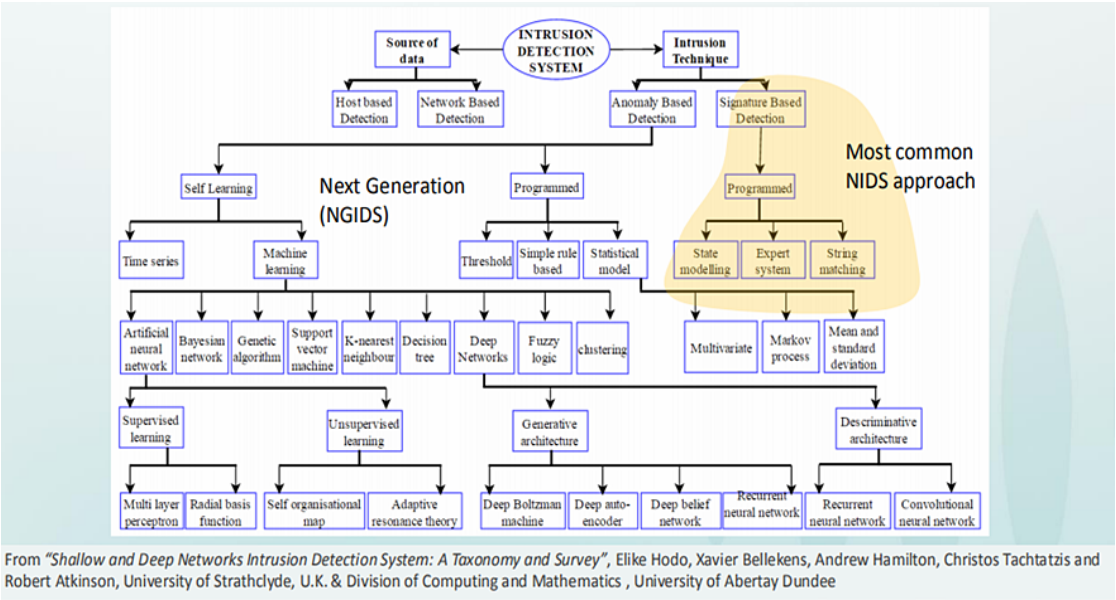
study would be concluded by a different researcher or from a different observer. The other issue is whether there is transparency in the way raw data was analysed and processed to draw conclusions.

Possible Outcomes

The expected accuracy rate for the research should be according to Table 3 below, which shows the international benchmark.

Table 3: Comparative Detection accuracy rate (%)

Classifier	Detection Accuracy (%)	Time taken to build the Model in seconds	False Alarm rate (%)
Decision Trees (J48)	81.05	**	**
Naive Bayes	76.56	**	**
Random Forest	80.67	**	**
SVM	69.52	**	**
AdaBoost	90.31	**	3.38
Mutlinomal Naive Bayes + N2B	38.89	0.72	27.8
Multinomal Naive Bayes updateable + N2B	38.94	1.2	27.9
Discriminative Multinomal Bayes + PCA	94.84	118.36	4.4
Discriminative Multinomal Bayes + RP	81.47	2.27	12.85
Discriminative Multinomal Bayes + N2B	96.5	1.11	3.0



From *"Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey"*, Elike Hodo, Xavier Bellekens, Andrew Hamilton, Christos Tachtatzis and Robert Atkinson, University of Strathclyde, U.K. & Division of Computing and Mathematics , University of Abertay Dundee

Fig.8: Landscape for Intrusion Detection

Analysis and Research Outcomes

The landscape for intrusion detection is shown on Figure 8 below. It must be noted that network traffic behaviour differs according to the service provision by each specific equipment with a known IP address By using sensibility analysis the knowledge representation model can be accomplished in order to avoid denial of service attacks (Bringas, P.B., and Santos, I., 2010, p.242). The simple rules for the

analysis of attack are shown on Figure 9 below. An alarm is triggered on the IDS in an anomaly-based intrusion detection if some type of unusual behaviour occurs on the network.

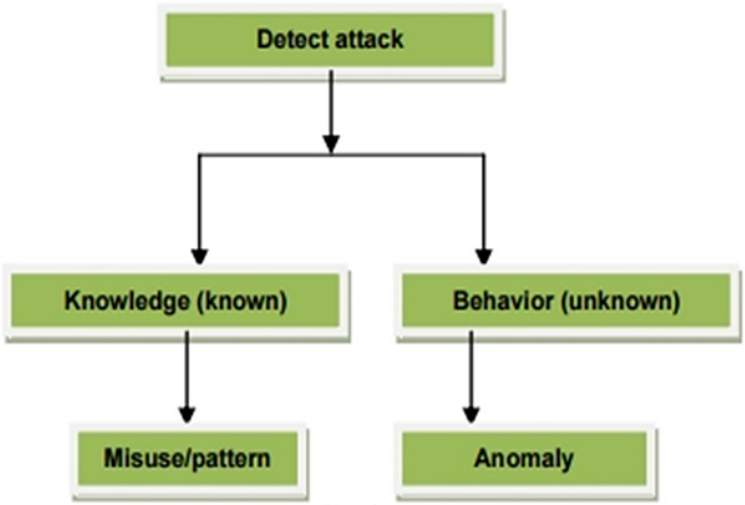


Fig.9: Analysis of Attack (Source: Murugan, S., and Rajan, M.S., 2014, p.2)

The research by Napanda, K., *et al.,*(2015) on the different Artificial Intelligence (AI) techniques highlighted the use of Machine Learning (ML), Neural Network and Fuzzy Logic to detect attacks on private networks. It must be noted that most of the Intrusion Detection Systems are signature based, and is it technically unfeasible to develop a perfect sophisticated Intrusion Detection System. An IDS can either be bifurcated as a Network IDS (NIDS) or as a Host IDS (HIDS). Network based IDS handles the analysis of the network traffic and distinguishes the unlicensed, illegitimate and anomalous behavior on the network. The IDS generally should capture packets traversing through the network using span port or network taps in order to detect and flag any suspicious activity (Napanda, K., *et al.,* 2015, p.1). A device specific IDS effectively detects malicious activity or anomalous behavior on the specific device.

An absolute cybersecurity remains a challenge these days of increasing Internet of Things (IoT). The Intrusion Detection System (IDS) are known for observation of the the network traffic, its analysis and identification of possible anomalies or unauthorized access to the network behavior, with some of the IDS responding to the intrusion to protect the computer network. However, there are several limitations and problems of the existing methods (Stefanova, Z.S., 2018, p.1). Arguably, there is a great challenge in providing a reliable way of protecting the network system or to trust the IDS. Administrators are required to regularly update their protection mechanisms in cases where specific weaknesses and limitations of the system have been recognized by the intruder, therefore challenging the detection system.

The use of wireless technology is increasing the vulnerability of networks and making them susceptible to cyber attacks (Stefanova, Z.S., 2018, p.2). The classical security measures have been proved to be grossly inadequate. There is need, therefore, to determine effective solutions for a dynamic and adaptive network defence mechanism. Neural networks trained for a specific problem domain can provide better solutions with the representative sets of training data (Stefanova, Z.S., 2018, p.5). According to Stefanova, Z.S. (2018, p.5), a majority of the IDS use ML classification problems solvable with supervised or semi-supervised learning models. However, one major limitation of the work done by Stefanova, Z.S. (2018, p.14) is on the analysis of the strategies and the solutions of the players based on the informational structure in cybersecurity.

An autonomous robotic vehicles can be attractive targets for cyber attacks to prevent them from navigating and of completing the mission of intrusion prevention. The limitation of such detection is confined to knowledge-based and vehicle-specific methods, which are applicable to only specific known attacks (Bezemskij, A., *et al.,* 2017, p.1). The attack vectors of the attack scenarios used by Bezemskij, A., *et al.,* (2017, p.2) is shown on Figure 10 below.

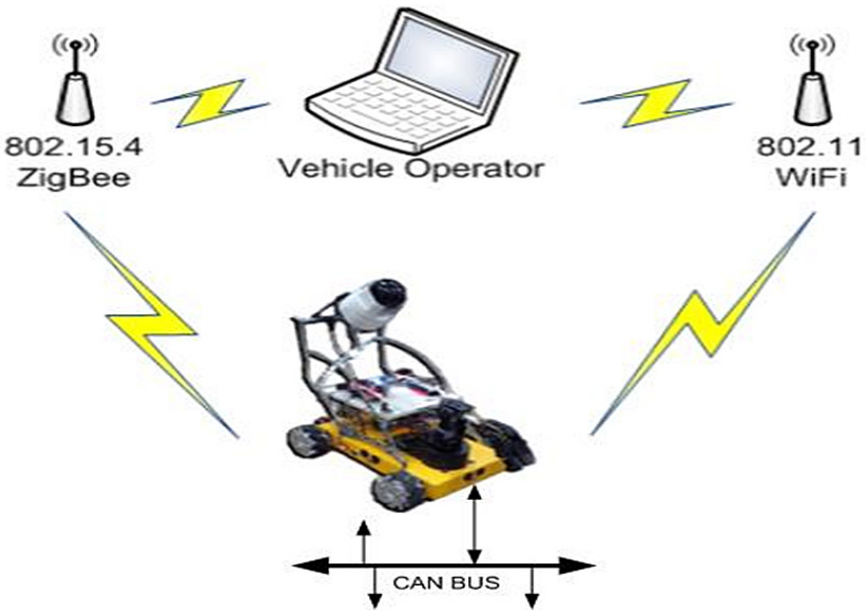


Fig.10: Attack vectors of the attack scenarios (Source: Bezemskij, A., *et al.*, (2017, p.2))

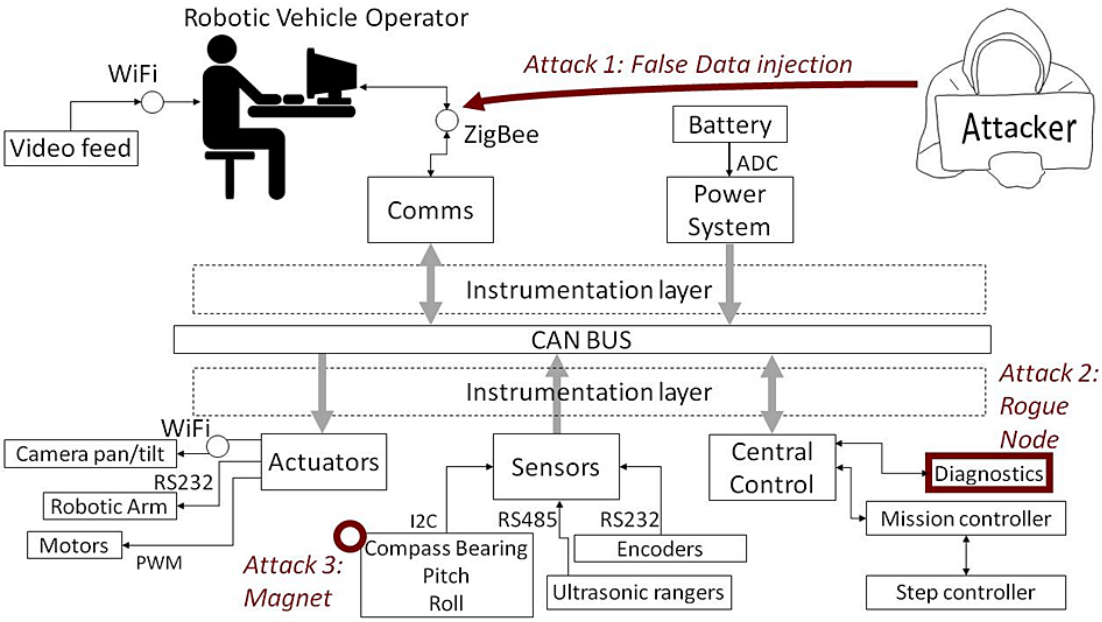


Fig.11: Attack vectors robotics experimental setup (Source: Bezemskij, A., *et al.*, (2017, p.4))

In this experiment, the system is allowed to undertake several missions by the robotic vehicle which is destined to reach on the ground with stochastic elements that divert the robotic vehicle testbed. The practical experimental setup for the attack vectors used is shown on Figure 11 below.

The methodology used by Bezemskij, A., *et al.,* (2017, p.3) is a self-learning approach which generalizes the sensor data into signatures and uses these signatures as the data source's unique description. Bezemskij, A., *et al.,*(2017, p.5) presented a Bayesian network which can receives real-time information from a vehicle's sensors, processes and communicates the modules in determining whether or not there is an attack. However, a limitation of this mechanism is its perfect performance only in low sampling frequency of one sample per second. A higher sampling frequency attracts lack of precise synchronisation between the heterogeneous data sources used..

Artificial Neural Networks (ANN) can be trained with the network traffic data to recognize the patterns in network data. Verification and distinguishing between intrusion and normal connections can be done by these neural patterns. An ANN transforms inputs to a set of searching outputs, through a set of simple processing units or nodes and connections between them (Sans Institute, 2011) (Alocious, C., *et al.,* 2014, p.3). Two types of training algorithms called supervised learning and unsupervised learning, are used by the neural network based intrusion detection systems. The supervised learning state is learning the desired output for a given input. The Multilevel perception (MLP) is the most commonly used form of supervised learning algorithms. Unsupervised neural network learning algorithm, represented as self organized maps, learns without specifying the desired output. The Inference Analyser is used to produce an IDS with a Bayesian Network as shown on Figure 12 below.

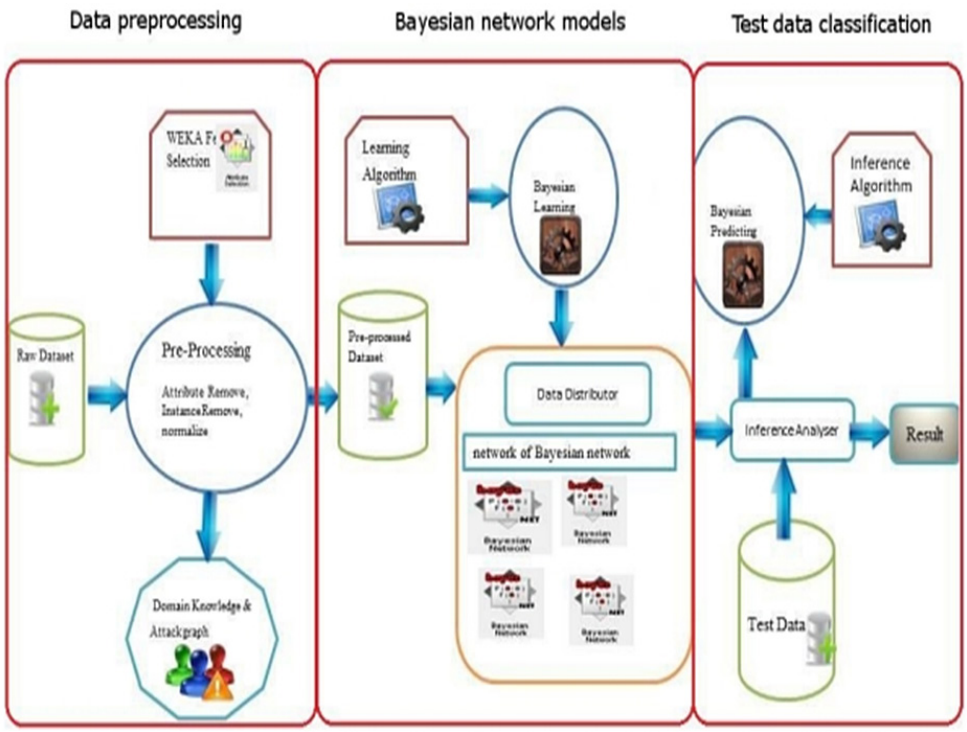


Fig.12: An IDS with a Bayesian Network and Inference Analyser

Profiles of network software behaviour can be built with Neural Networks and distinguish between normal and anomalous/malicious software behavior (Napanda, K., *et al.,* 2015, p.2). The use of Neural

Networks in Intrusion Detection enables us to classify between malicious and safe networks. An ANN comprises processing units, nodes, and connections between them.

When solving complex problems one can use Fuzzy Logic which involves a fuzzy set of elements that can vary from 0 to 1 (Napanda, K., *et al.,* 2015, p.3). However, unlike Boolean sets of) and 1, there is no crisp value, although there is a perfect representation of the membership of the elements.

Machine Learning (ML), Neural Network and Fuzzy Logic can detect and prevent cyber attacks on private networks. The current trend is to use Expert Systems, Neural Networks, Genetic Algorithms, Fuzzy Logic and others. Expert IDS can recognize and learn through patterns. According to Zekrifa, D.M.S. (2014, p.15), most of the anomaly detection systems face a major challenge in the great capability in detecting unknown or zero-day vulnerabilities where they suffer from a major deficiency in their high false alarm rate. The two major causes of the problem are that there is a lack of a training data set that covers all the legitimate areas, and that abnormal behavior is not always an indicator of intrusions.

Existing techniques for preventing intrusions often start with encryption and firewalls, then followed by Intrusion Detection System (IDS) technology can detect unauthorized access and abuse of computer systems from both internal users and external offenders (Tran, T.P., 2009, p.iv). Artificial Intelligence (AI) technologies such as Artificial Neural Networks (ANN) have been adopted to improve detection performance. The true power and advantage of ANN lie in its ability to represent both linear and non-linear underlying functions and learn these functions directly from the data being modeled. However, ANN is computationally expensive due to its demanding processing power, and so the network is unable to extrapolate accurately once the input is outside of the training data range (Tran, T.P., 2009, p.iv). These limitations challenge security systems with low detection rate, high false alarm rate and excessive computation cost. Tran, T.P. (2019) developed a novel Machine Learning (ML) algorithm to alleviate those difficulties of conventional detection techniques used in available IDS.

Table 4 below shows a comparison of the data mining techniques that can be used in intrusion detection.

Table 4: Advantages and disadvantages of data mining techniques (Source Almutairi, A. (2016) p.43)

Technique	Advantages	Disadvantages
Genetic Algorithm	- Finding a solution for any optimization problem. - Handling multiple solution search spaces.	- Complexity to propose a problem space. - Complexity to select the optimal parameters - The need to have local searching technique for effective functioning
Artificial Neural Network	- Adapts its structure during training without the need to program it.	- Not accurate results with test data as with training data
Naive Bayes Classifier	- Very simple structure. - Easy to update.	- Not effective when there are high dependency between features.
Decision tree	- Easy to understand - Easy to implement	- Works effectively only with attributes having discrete values. - Very sensitive to training sets, irrelevant features and noise.
K Mean	- Very Easy to understand. - Very simple to implement in solving clustering problems.	- Number of clusters is not automatically calculated. - High dependency on initial centroids.

The efficiency of data mining techniques ought to be optimized and enhanced in the quest for intrusion attack classification. Ajayi, A. *et al.,* (2013, p.239) evaluated the performance of the five popular data mining algorithms and these are Decision trees, Naïve bayes, Artificial neural network, K-nearest neighbor algorithm and Support vector machines. The pros and cons of each algorithm using the NSL-KDD dataset are shown on Table 5 below.

Table 5: Performance of Support Vector Machines, Artificial Neural Network, K-Nearest Neighbour, Naive-Bayes and Decision Tree Algorithms

Parameter	SVM	ANN	KNN	NB	DT
Correctly classified instances	24519	24123	25051	22570	25081
Incorrectly classified instances	673	1069	141	2622	111
Kappa Statistic	0.9462	0.9136	0.9888	0.7906	0.9911
Mean Absolute Error	0.0267	0.0545	0.0056	0.1034	0.0064
Root Mean Squared Error	0.1634	0.197	0.0748	0.3152	0.0651
Relative Absolute Error	5.3676%	11.107%	1.1333%	20.7817%	1.2854%

An intrusion detection system monitors computer systems and networks to determine if a malicious event (i.e., an intrusion) has occurred, and each time a malicious event is detected, the IDS raises an alert (Bolzoni, D., 2009, p.13). Consequent to this, we can possibly get a true positive (TP), a false positive (FP), a true negative (TN) or a false negative (FN) which occurs when no alert is raised but a real intrusion attempt takes place. However, Bolzoni, D., (2009) addressed the problems of reducing false positives by allowing a user to interact with the detection engine and raising classified alerts generated by an Anomaly Based Signature (ABS). The advantages and disadvantages of ABSs and SBSs are summarised on table, Table 6, below.

Table 6: Advantages and disadvantages of ABSs and SBSs models (Source: Bolzoni, D., 2009, p.27).

Detection model	Advantages	Disadvantages
Signature-based	Low false positive rate Does not require training Classified alerts	Cannot detect new attacks Requires continuous updates Tuning could be a thorny task
Anomaly-based	Can detect new attacks Self-learning	Prone to raise false positives Black-box approach Unclassified alerts Requires initial training

An IDS must keep up with the amount of data and number of involved networking components and devices that process the data. Developing a cloud-based intrusion detection system requires additional requirements due to its complex architecture and integrated services that interact together as well as with outside services. According to Aljebreen, M.J. (2018, p.18), a cloud based intrusion and detection system has the following minimum requirements:

- Handle large-scale, dynamic multi-tiered autonomous computing and data processing environments
- Detect a variety of attacks with minimal False

Positive Rates
- Detect intrusions as they occur
- Self-Adaptive Autonomically, where the CIDS should adapt to changes in configurations as the computing resources are dynamically added and re?moved.
- CIDS Scalability which can handle a large number of network nodes.
- Be deterministic, where the CIDS should maintain the acceptable service?level agreement (SLA), be reliable, have high uptime service as well as maintaining minimum overhead.
- Synchronize the autonomous CIDS, whereby the collaborated intrusion detection systems must be synchronized in order to detect attacks in real-time.

The intrusion detection situation can be considered as a classification problem.

Challenges and Future Direction

Cyber attacks are advancing rapidly and outpacing the technical measures in cybersecurity that deploy new signatures to detect these new attacks (Berman, D.S., *et al.,* 2019). This challenging situation in combination with advances in machine learning (ML) presents unlimited opportunities to apply neural network-based deep learning (DL) approaches to cyber security applications to detect new variants of malware and zero-day attacks. The future direction of research in this area should the cascading connection of malicious activities throughout an attack lifecycle and the metrics for evaluation of DL performance. However, new datasets are required to develop new DL approaches for cybersecurity systems.

Conclusion

An intrusion detection system monitors and determines whether or not a malicious event has occurred, and raises an alert each time a malicious event is detected (Bolzoni, D., 2009, p.13). The main research question was: Which artificial intelligence paradigm is most effective in developing a Cybersecurity system than can handle a higher degree of complexity? The first step in Network Security is to redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. It must be noted that network traffic behaviour differs according to the service provision by each specific equipment with a known IP address.

Intrusion detection and prevention systems (IDPS) include all protective actions or identification of possible incidents, analysing log information of such incidents, how to block them in the beginning itself and generate reports for the concern of security personnel (Umamaheswari, K., and Sujatha, S., 2017, p.1). The complexity of cyber-physical systems (CPS), the roles and responsibilities of the humans that interact with them, and the cyber-security of these highly interconnected systems now requires a resilient CPS (Ghafouri, A., 2018, p.1). According to Ghafouri, resilient CPS provide interdisciplinary solutions for problems such as how to tailor the control system to enable it to respond to disturbances quickly and efficiently, how to better integrate widely distributed CPS to prevent faults that result in disruptions to operations of critical infrastructure, and how to design cyber-security protection mechanisms so that the system defends itself from cyber-attacks by changing its behaviors.

The Artificial Neural Networks (ANN) have been found to be quite effective, especially when they use multilayer perceptrons, as was used by Aljebreen, M.J. (2018, p.32) in intrusion detection. The multilayer perceptron learns the model from the training data using an algorithm called backpropagation. The Error data at the output layer is back propagated to earlier ones, which allows incoming weights to these layers to be updated.

Acknowledgement

I deeply appreciate the Atlantic International University for supporting this research work as part of my Doctor of Science degree in Computer Science.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of interest

There is no conflict of interest associated with this publication.

References

1. Acs, (2016).Cybersecurity: Opportunities, Threats and Challenges.
2. Africa Cybersecurity Report, (2016).
3. https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
4. Ajayi, A., Idowu, S.A., and Anyahie, A.A., (2013). Comparative Study of Selected Data Mining Algorithms Used For Intrusion Detection, *International Journal of Soft Computing and Engineering (IJSCE)*, ISSN: 2231-2307, Volume-3, Issue-3, July 2013, p.237-241.
5. Aljebreen, M.J., (2018). Towards Intelligent Intrusion Detection Systems for Cloud Computing, Ph.D. Dissertation, Florida Institute of Technology, 2018.
6. Almutairi, A., (2016). Improving intrusion detection systems using data mining techniques, Ph.D Thesis, Loughborough University, 2016.
7. Alocious, C., Abouzakar, N., Xiao, H, and Christianson, B., (2014), Intrusion Detection Framework for Cyber Crimes using Bayesian Network, https://www.researchgate.net/publication/272999966_Intrusion_Detection_Framework_for_Cyber_Crimes_using_Bayesian_Network
8. Al Hogail, M., (2015). How is the ministry fostering public-private partnerships (PPPs) with local private developers?, https://oxfordbusinessgroup.com/interview/right-home-obg-talks-majed-al-hogail-minister-housing
9. Angelini *et al.,* (2017).CRUMBS: a Cybersecurity Framework Browser.
10. Apruzzese, G; Colajanni, M.; Ferretti, L.; Guido, A.; & Marchetti, M.(2018). "On the effectiveness of machine and deep learning for cyber security," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 371390.
11. Azzalini, A., and Scarpa, B., (2012), Data analysis and data mining : an Introduction, Oxford University Press, Inc., ISBN 978-0-19-976710-6.
12. Berman, D.S., Buczak, A.L., Chavis, J.S., and Corbett, C.L. (2019). "Survey of Deep Learning Methods for Cyber Security", Information 2019, 10, 122; doi:10.3390/info10040122
13. Bezemskij, A., Loukas, G., Gan, D., and Anthony, R.J., (2017). Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian Networks, 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 21-23 June 2017, IEEE, United Kingdom, https://ieeexplore.ieee.org/document/8276737
14. Bolzoni, D., (2009). Revisiting Anomaly-based Network Intrusion Detection Systems, Ph.D Thesis, University of Twente, The Netherlands, ISBN: 978-90-365-2853-5, ISSN: 1381-3617, DOI: 10.3990/1.9789036528535,
15. Bringas, P.B., and Santos, I., (2010). Bayesian Networks for Network Intrusion Detection, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4, InTech, Available from: http://www.intechopen.com/books/bayesian-network/bayesian-networks-for-network-intrusion-detection
16. Concierge, (2018). Concierge Security Report. Cybersecurity: Trends from 2017 and Predictions for 2018.
17. Cornmen, T.H, Leiserson, C.E, Rivest, A.L, Stein, C. (2009). 3rd ed. Introduction to Algorithms. Cambridge: MIT Press.
18. Crewell, J.W., (2014). Research Design: Qualitative, quantitative and mixed methods .4rd edition, Sage Publications,Inc.
19. Demir, N., and Dalkilic, G., (2017). Modified stacking ensemble approach to detect network intrusion, *Turkish Journal of Electrical Engineering & Computer Sciences*, Accepted/Published Online: 15.11.2017, http://journals.tubitak.gov.tr/elektrik/
20. European Union Agency for Network and Information Society (2017) https://openarchive.cbs.dk/bitstream/handle/10398/9524/EvaluationofENISA-FinalReport.pdf?sequence=1
21. Fehling, C., Leymann, F., Retter, R., Schupeck, W., Arbitter, P. (2014). Cloud Computing Patterns. Fundamentals to Design, Build, and Manage Cloud Applications. Springer-Verlag Wien .

22. Flick, U., (2013). The SAGE Handbook of Qualitative Data Analysis: Mapping the Field, New York, 2013.
23. Gcaza, N., Solms, R. Von, & Vuuren, J. Van. (2015). An Ontology for a National CyberSecurity Culture Environment. *In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2015) (1-10).
24. Gercke, M. (2012). 'Cybercrime Understanding Cybercrime', Understanding cybercrime: phenomena, challenges and legal response.
25. Ghafouri, A., (2018). Resilient Anomaly Detection in Cyber-Physical Systems, Ph.D. Dissertation, Faculty of the Graduate School of Vanderbilt University, February 2018.
26. Karimpour, J., Lotfi, S., and Siahmarzkooh, A.T., (2016). Intrusion detection in network flows based on an optimized clustering criterion, Turkish Journal of Electrical Engineering & Computer Sciences, Accepted/Published Online: 17.07.2016, http://journals.tubitak.gov.tr/elektrik
27. Kothari, C., (2004). Research Methodology Methods and Techniques, 2nd Edition. New Age International Publishers.
28. Kpmg, (2018).Clarity on Cybersecurity. Driving growth with confidence.
29. MacAfee, (2018). https://www.mcafee.com/consumer/en-sg/store/m0/catalog.html
30. Malyuk and Miloslavskaya, (2016). Cybersecurity Culture as an Element of IT Professional Training, TBA.
31. Murugan, S., and Rajan, M.S., (2014). Detecting Anomaly IDS in Network using Bayesian Network, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 16, Issue 1, Ver. III (Jan. 2014), PP 01-07, www.iosrjournals.org
32. National Institute of Standards and Technology, (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
33. Napanda, K., Shah, H., and Kurup, L., (2015). Artificial Intelligence Techniques for Network Intrusion Detection, I*nternational Journal of Engineering Research & Technology (IJERT),* ISSN: 2278-0181, IJERTV4IS110283 www.ijert.org, Vol. 4 Issue 11, November-2015.
34. Nielsen, R. (2015). CS651 Computer Systems Security Foundations 3d Imagination Cyber Security Management Plan, Technical Report January 2015, Los Alamos National Laboratory, USA.
35. Norton Symantec (2017) '2017 Norton Cyber Security Insights Report - Global Results', p. 2018.
36. Oxford English Dictionary (2019). Oxford: Oxford University Press. Available at: https://en.oxforddictionaries.com.
37. Saunders, M.N.K., Thornhill, A., and Lewis, P., (2009). Research Methods for Business Students (5th Edition),Publisher: Pearson; ISBN-13: 978-0273716860, ISBN-10: 0273716867, https://www.amazon.com/Research-Methods-Business-Students-5th/dp/0273716867
38. Stefanova, Z.S., (2018). "Machine Learning Methods for Network Intrusion Detection and Intrusion Prevention Systems", Graduate Theses and Dissertations, 2018, https://scholarcommons.usf.edu/etd/7367
39. Sharma, R. (2012). Study of Latest Emerging Trends on Cybersecurity and its Challenges to Society. *International Journal of Scientific and Engineering Research* .Vol 3 Issue 6, June 2012.
40. Stallings, W., (2015). Operating System Stability. Accessed on 27th March, 2019. https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf
41. Symantec Annual Report (2016), https://s1.q4cdn.com/doc_financials
42. Tran, T.M., Ko, D.W., Ryul, C., and Dinh, H., (2019). A bayesian network analysis of reforestation decisions by rural mountain communities in Vietnam, Forest Science and Technology, DOI: 10.1080/21580103.2019.1581665.
43. Tran, T.P., (2009). Innovative machine learning techniques for security detection problems, Ph.D. Dissertation, University of Technology, Sydney, Australia, 2009.
44. Truong, T.C; Diep, Q.B.; & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry* 2020, 12, 410.
45. Umamaheswari, K., and Sujatha, S., (2017). Impregnable Defence Architecture using Dynamic Correlation-based Graded Intrusion Detection System for Cloud, Defence Science Journal, Vol. 67, No. 6, November 2017, pp. 645-653, DOI : 10.14429/dsj.67.11118.
46. United Nations Economic Commission for

Africa. (2014).Tackling the challenges of cybersecurity in Africa.
47. Yedaly, M. and Wright, B. (2016) 'Cyber Crime & Cyber Security Trends in Africa', Symantec.
48. YU, J., Chang, G.K., Kooning, A.M.J, and Ellinas, G., (2009). Radio-over-optical-fiber Networks: Introduction to the feature issue, *Journal of Optical Networking,*
49. Williams, B. T., (2014). The joint force commander's guide to cyberspace operations. Joint Force Quarterly, 73(2), 12–19. Retrieved from http://ndupress.ndu.edu/ Portals/68/ Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf.
50. Zekrifa, D.M.S., (2014). Hybrid Intrusion Detection System, Ph.D Thesis in Computer Science, School of Information Technology & Mathematical Sciences, 2014, University of South Australia, https://tel.archives-ouvertes.fr/tel-01584217.