Sri Lanka Institute of Information Technology

Preserve Cybersecurity by Using Artificial Intelligence based Intrusion Detection Techniques

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20021870	Dilshan K. N

Date of submission

28th May 2021

Table of Contents

Abstract

The last decades were the golden peak time of Artificial Intelligence [AI]. The Majority of sectors like finance, health care, Computer network security, switch Artificial Intelligence-based automation systems to increase productivity, accuracy, security of their services. With the current technical evolution, countless zero- day threat coming to cybersecurity in every single day. In present hackers and other intruders are making use of cutting-edge technologies to develop new cyberattacks on large organizations to small Co-operations. Over the time cybersecurity researchers developed various Artificial Intelligence based security tools to address such issues and testing those tools by using various security systems to reduce ever increasing cyberattacks on their systems. Finally, proper security protocols have been developed with the help of improved neural networks and deep learning concepts.

Researchers identify the essentiality of identifying the existing types of cyberattacks and threats prior to designing an Intrusion detection system. Then need to determine how those existed threats and attacks were mounted against computer systems. Core compartment of Intrusion detection systems developed based on Artificial intelligence deep learning, neural networks, and expert system concepts. After deploying those expert systems, they can determine if the analyzed document was either legitimate or malicious without any human interaction. This technique may lead to identifying ever increased threat recognizing including malware, phishing attacks, zero-day vulnerabilities, and many more. Intrusion detection systems are basically used as a passive monitoring device. It may notify the security operation center of the system when if any security breach or potential threat occurs. by examining the security alerts, system admins can perform necessary actions.

Keywords: Artificial Intelligence [AI], Cybersecurity, Neural Network, Threats, Malware Deep learning, Expert systems, Phishing Attack, Zero-day Vulnerability, Cybercriminals, Intrusion Detection System [IDS], Security Alert

1. Introduction

What is a Computer? As we all know, a Computer is a machine, that consists of several integrated hardware, Operating Systems, and other applications to perform a sequence of arithmetic or logical operations automatically. Due to the rapid growth of computer technologies, modern computers able to complete more complex, tedious tasks in milliseconds. Because of that most likely computers are used as control systems in a wide range of industrial and consumer services to increase their throughput.

Over 80% of people who currently living in the world use computers to accomplish their day-to-day life matters. As same as, connectivity defines the world of modern. In the last decade, social networks, mobile devices, the Internet have entirely changed society [3]. With help of the above technologies, people can be anywhere in the world today and connect with any others in real- time.

With greater power there must also come great responsibility like sense, with use of great computing power there must also come the computer security or the cybersecurity behind on it. When the usage of computers became high, users try to find their privacy in the computer generic world. More or likely the same, some sort of computer users felt in other intentions. As human nature, they were getting curious about the others business. Then those types of users try to figure out the new methods to jump into someone else's computers to view or retrieve the data which would normally prohibit to access. Then the Term Hacker or Intruder introduce to name such kind of computer users.

Title 'hacker' is typically used in computer generic as to address the computer master minds who use potential skills to achieve a goal or overcome an obstacle, within a computerized system by non-standard means [2]. Normally hackers make use of their

technological abilities to sneak into computers to access unauthorized resources that would not be able for access legally. Furthermore, law enforcement authorities perform hacking by the legitimate figure in legal situations to collect evidence.

To reduce or prevent unauthorized activities for computer systems, security protocols being implemented but most of the implemented security protocols fail to accomplish their duties. When examine the past few years, cyber attackers like black hat hackers introduce various new cyber weapons to override the modern security implementations. Without a proper mechanism to protect against such intrusions, users' privacy in great danger.

Despite all the achievements and miracles, cybersecurity executives face many complex technical challenges. The increasing of the threats and complex and frequent attacks put their lives in a miserable and defensive position [1]. Due to the recent critical security breaches, the demand for better security and protection has been rapidly increased but there are not enough cybersecurity professionals in the action. The lack of skill level and shortage of security professionals further downgrade the recent fulfillment of computer security. To sort out all kinds of security issues Artificial Intelligence was introduced into cybersecurity. With the use of Artificial Intelligence, security professionals able to detect, prevent, mitigate and predict all kinds of threats before even they perform. Because of that modern era of cybersecurity heavily rely on the main aspects of Artificial Intelligence.

In this report under the 'Preserve Cybersecurity by using Artificial Intelligence Threats Detection techniques' initially we try to describe how the intrusion detection techniques evaluate, concerning the core compartment of Artificial Intelligence. the next part of the report describes the future development of the threat identification and intrusion detection techniques and finally finishes the report with a conclusion, which is based on the small research against the field.

2. Evolution of the topic

Initially, Artificial Intelligence and Cybersecurity were treated as two different sections. Researchers who use Artificial Intelligence, create automation programs, while cybersecurity researchers looking for patch the security leakages on the systems. Suddenly those fields overlap each other with the time. Few decades back, web proxies, anti-virus software, firewalls were used as security measures in traditional organizational systems. However, with digitalization, there has been a dynamic shift in the cyber threat landscape [7] because of that the majority of companies deploying artificial intelligence and machine language tools for better security but such kinds of tools never developed overnight.

As daily operations grew progressively, computer system security dependent upon levels of access to those systems, clear visibility into user activity, and shared use of information systems were needed to control firmly and safely [8]. At that time demand of proper intrusion detection tools getting higher. It is the unrelenting active attempts in detecting the presence or discovering of intrusive activities. Basically, Intrusion Detection (ID) refers as it relates to network infrastructure and computers encompasses a far broader scope. It refers to all processes used in discovering unauthorized uses of computer devices or networks. This is achieved through specifically designed software with the sole purpose of detecting unusual or abnormal activity [9].

On 31st August 1955, the term "Artificial Intelligence [AI]" is coined in a proposal for a "2 month, 10 man study of artificial intelligence" provided by Nathaniel Rochester, Claude Shannon, Marvin Minsky and John McCarthy. The workshop, which took place a year later, in July to August 1956, is generally considered as the official birthdate of the new field [3] but lack of computational power and lack of funds were the biggest concerns that felt in researchers.

From 1958 to 1980, AI prospered. Computers built with increased memory capacity, that help to store more data inside the computer. Also, computers provide more accessible

facilities, more efficiency processing and computers getting cheaper. At that time John McCarthy develops a famous programming language called 'Lisp' which is used in artificial intelligence research. Machine learning algorithms also deploying on that time and people had a proper understanding about, which algorithm could resolve their problem [4]. With the immigration of AI Neural Networks, computers able to recognize the patterns based on two layers of the learning network. Natural language understanding computer program called 'STUDENT', was built by Carl Djerassi, Joshua Lederberg Edward Feigenbaum and Bruce G. Buchanan. It also considered as the first expert system that use automated problem-solving and decision-making features. first general-purpose mobile robot – SHAKEY, WABOT1 - first anthropomorphic robot, The invention of first automation the driverless Mercedes car, Rollo Carpenter's JABBERWACKY chat-bot and other expert systems like MYCIN, XCON can consider as the landmark innovations on that period of time.

Artificial intelligence is a term used to describe a machine that is capable of making intelligent decisions. We mostly see people using the terms Artificial intelligence, deep learning and machine learning synonymously. However, deep learning is a subset of machine learning, and machine learning is a subset of AI [4]. Somehow in the early stages, the majority of the people denatured to believe that the researchers were able to construct such kind of fully intelligent machines but years of research and testing, accomplish the miracle. Some associations like 'Defense Advanced Research Projects Agency (DARPA)' and the Japanese government continuously funding researchers. As a result, Artificial Intelligence became the fourth industrial evaluation of the modern world.

At 1971, BBN Technologies researcher Bob Thomas invented the self- duplicating worm which called as Creeper virus/ worm. It is an experimental program and that was not built for any intentional leverages. Creeper corrupted DEC PDP-10 computers operating on the TENEX operating system by messing around the installed printers, displaying the message "I'm the creeper, catch me if you can!" [10]. That worm generally refers as the very first computer virus. In 1986, the first computer-based malware, known as "Brain," was launched. Primary virus or malware basically developed as a boot loader programs

and they built to infect the user files and distribute using floppy disk. In 1988, viruses start to distribute alone with the internet. The Morris worm consider as the first malicious programs which distributed via the internet. The virus Jerusalem which is appear as Denial of service (DOS) type virus.

The increased regulation violations or breach of computer security access, Initially, the idea of the intrusion detection came from a "How to use accounting audit files to detect unauthorized access'' report which published in 1980, by United State Air Force, Defense Science Board Task Force on Computer Security member and researcher James P. Anderson. During that time, the U.S Air Force had the difficult task of providing shared use of their computer systems, which contained various levels of classifications in a need-to know environment with a user base holding various levels of security clearance [9]. The process of recognizing acts that attempt to violate a resource's overall integrity and confidentiality is known as intrusion detection. Intrusion detection's purpose is to discover intruders who try to break into systems and compromise security controls.

In 1984 - 86, SRI International has developed a design of an expert system for real-time intrusion detection (IDES) based on Artificial neural networks. This system is a stand-alone system that monitors and flags suspicious events on one or more monitored computer systems. IDES keeps track of remote hosts, entire systems, individual users, and groups, and detects potential security breaches by both outsiders and insiders as they happen. IDES adaptively learns users\' behavior patterns over time and detects behavior that deviates from these patterns [11]. Additionally, to that those systems, encodes known system vulnerabilities and intrusions by performing rule-based expert system techniques which may help to detect intrusion as well as the unauthorized use of authorized users.

While considering the Artificial Neural Networks, that consist of nodes called artificial neurons, which work as same as the biological neurons. Those neurons connect one to another by transmitting electrical signals also artificial neurons aggregated into different layers. Initially, Artificial Neurol Networks learn by processing examples. Particular network processing examples with predefined inputs and outputs stored inside the data

structure of the network and then expected to have targeted output but the final processed output may differ from the targeted output. After coming with a significant number of adjustments, now such kinds of networks capable of producing outputs with high accuracy.

David Rumelhart and John Hopfield introduce the Deep learning concept, that is essentially a neural network which contains numerous layers of interconnected nodes in its structure. Every layer of the network, build using a process called forward propagation. This means each layer built upon the below layers to optimize and refine the categorization or prediction. Those neural networks mimic to simulate the behavior of the human's brain ability to “learn, recognize, classify and describe” objects from large amounts of data.

There are two main layers in deep learning neural networks, usually called as visible layers. While the input layer provides the data for processing and the output layer is the place where the end classification or prediction is made. A process called backpropagation uses algorithms, like gradient descent, to calculate errors in predictions and then adjusts the biases and weights of the function by moving backward through the layers in an effort to train the model. Together, backpropagation and forward propagation allow a neural network to correct for any errors and make predictions accordingly [6]. Those predictions and error detections or error corrections capability of neural networks consider as core compartments of the Intrusion detection systems.

After the successful start of the intrusion detection systems, in the period of mid 80's Suddenly United States government starting supply funds to security researchers to build more systems. Because of that projects like Multics Intrusion Detection and Alerting System (MIDAS), Discovery, Intrusion Reporter (NADIR), Network Audit Director, and Haystack were all developed to detect intrusions.

At that time stage, intrusion detection systems categorize by considering the model of intrusion and the data source. Host-based intrusion detection systems were created to detect intrusion and audit data from a single host under the data source intrusion detection systems category. Multi-host-based systems are used to identify intrusions and audit data, that came

from many hosts. To detect an intrusion, network-based systems examine network traffic data as well as audit data which came from one or more hosts. When considering the model of intrusion systems, an anomaly detection model is a type of intrusion detection system that looks for activity that differs from a system's or user's typical behavior to detect intrusions. Also, Misuse detection models are used by intrusion detection systems to detect intrusions by looking for activity that corresponds to known system vulnerabilities or known intrusion techniques.

Malware propagation grew easier as computer networks expanded and use increased in the early half of the 1990s, resulting in an increase in volume. Certain types of malware proliferated as technologies became more standardized. The increased adoption of email aided the distribution of macro viruses (which enable malware to be spread via email attachment) that exploited Microsoft Office products. By the mid-1990s, businesses became increasingly affected, due in large part to macro viruses, meaning propagation had become network-driven [13].

In 1995, company Wheelgroup was formed to create security product that can be sold and its initial product called as a Netranger. Initial prototype of Netranger was developed by the United State Air Force. That tool capable enough of scanning the traffic to analyze the misuse and also that providing details of the intrusion and real- time alarm if any intrusion occurs in the network. At 1998 Cisco brought Wheelgroup company and add that company as an integral part of Cisco's security architecture.

Christopher Klauss and Thomas Noonan founded Internet Security Systems Inc (ISS) in 1994. Then the initial prototype of the "Internet Scanner" was invented and released in 1996 by Christopher Klauss. Soon after that, the Internet Security Systems Inc (ISS) released the tool called 'RealSecure 1.0' to increase network security with real-time attack recognition. Initially, that tool introduces to deploy on Windows NT 4.0.

In 1998, Marty Roesch created the free tool 'Snort,' which can be used as a network-based or host-based intrusion detection system, as well as a lightweight system. Initially, it was developed with limited capabilities and that can only work for UNIX systems. After

appearing of Y2K bug, also called the Millennium Bug or Year 2000 bug, a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000 [12], version 1.5 of Snort was released. Performing real-time packet analyzing and logging were highlighted features of that version 1.5.

During this time detection systems can only detect known attacks or signatures of exploits. Most available detection systems are knowledge-based or behavior-based in origin. Basically, signatures were not written to identify the vulnerabilities which mean, when if an attacker discovered a vulnerability, that vulnerability can be exploited in many different ways. That may cause intrusion detection system vendors to write different exploit signatures to overcome with new exploits. However, those systems must need to be updated continually their databases with new knowledge to detect new attacks but having the most signatures was useless to overcome with new exploits, use of other methods such as string matching, pattern matching, heuristic-based detection, and anomaly detection gain more benefitable outcomes.

To address such kinds of issues, researchers have been organized an annually workshop. In that workshop broad range of subjects such as previous experiences, intrusion detection systems and Law, Modeling Attacks, Anomaly Detection was cover and subject-related information was sharing among researchers. The agenda of each workshop differs from every year and find novel solutions for emerging and difficult challengers are consider as main objectives.

With a arrival of new threat like SQL Injection and cross-site scripting, people switching to intrusion detection systems for better security rather than firewalls. In that time more than 3500 signatures were stored in databases but those large amounts of signatures, reduce the efficiency of intrusion detection systems. Tcpdump was used by the Audit Data Analysis and Mining (ADAM) IDS to create rule profiles for categorization in 2001.

2005 upwards, speed of the networks increased in Gigabyte per second [Gbps], as a result, manufactures of intrusion detection systems had to offer their products which compatible with that network speed. Increased network speed allows intrusion detection systems to monitor more segmented networks, web farms, etc. To overcome with Distributed Denial of Service (DDoS) attacks, researchers create protection by using an intelligent agent. An intelligent agent (IA) is an autonomous entity that sees through sensors and follows up on a domain utilizing actuators and coordinates its action towards accomplishing objectives [14]. In order to achieve their goals, an intelligent agent can also learn or use information. They can adapt to real-time, learn new things quickly through interactions with the environment, and store and restore memory-based models.

Viegas created an anomaly-based intrusion detection engine in 2015 for Internet of Things (IoT) System-on-Chip (SoC) applications (IoT). That engine was created utilizing machine learning methods for anomaly detection, ensuring energy efficiency in the construction of Decision Tree, Naive-Bayes, and k-Nearest Neighbors classifiers in an Atom CPU and their hardware-friendly implementation in an FPGA. In simple terms, this engine can measure software and hardware energy consumption by implementing classifiers in both components. This anomaly-based intrusion detection engine became the first engine, who can measure the energy usage of each feature used to classify network packets, as implemented in both hardware and software.

Some artificial intelligence related defense systems like Bitdefender and Palo Alto Networks have been implemented advanced machine learning algorithms into their systems to address new threats over the predefined operating procedures. Bitdefender employs predictive modeling to generate predictions, judgments, and detect patterns in order to learn how threats act and what they will look like in the future [18]. When considering Palo Alto Networks' PAN-OS 7.0, which is developed to identify address more complex network- based security threats.

By using artificial intelligence to actual cyber defense datasets, the Canadian Institute for Cybersecurity (CIC) generated the most recent and powerful intrusion detection dataset

for Amazon online services in 2018. (CSE-CIC-IDS2018). This system consists of artificial neural networks and it has provided an excellent Accuracy score performance of The average area under the Receiver Operator Characteristic (ROC) curve is 0.999, real-time network data analysis and the average False Positive rate is 0.03 [13]. That system can be deployed into and network traffic analysis and many other systems to detect botnet activities.

Modern detection tools come with a detailed graphical user interface (GUI) that includes, real-time updated graphs and charts. That added feature is very helpful to the non-technical oriented people. In addition to that, they had the ability to track front end protocols like HTTP, DNS, FTP, POP as well as capable of monitoring low level activities of the protocols like TCP, IP, UDP, ICMP, and TLS. And try to increase their productivity and accuracy by integrating with many other third- party analyzing tools such as Network Miner, Sguil, Snorby, ELSA, Squil, Xplico, Kibana, and BASE.

.

.

3. Future developments in the area

In the same way that Intrusion Detection Systems identify as a core part of systems defense, Artificial Intelligence [AI] plays a key role in cybersecurity services. More likely the same next generated intrusion detection systems had to address various kinds of cyber threats. With the rapid development of artificial neural networks and deep learning technologies, hackers same as the security exclusives use autonomous tools to overcome with each other [one makes the other better]. Modern day hackers searching vulnerabilities by using automated scripts, that may crawl through databases and digital addresses to find exploitable vulnerabilities.

Due to the rapid growth of the inside and outside cyber- attacks, the Global security market share of Intrusion Detection Systems will also expect to be increased. The market share of Intrusion Detection Systems, mainly divided based on their deployment model, service and, type. According to the Global Market Insights Inc, recently published research Intrusion Detection System (IDS) Market size estimated at USD 3 billion in 2018 and is growing at a CAGR of over 12% between 2019 and 2025 [19]. In addition to that 20% of the market share belong to network- based Intrusion Detection Solutions like Bro, OSSEC, Snort, Suricata, Security Onion.

The majority of modern attacks perform by using Malware. Malicious websites, Phishing/ Spear- phishing techniques used to distribute malware from attacker to target system. Malware is generally malicious software which, might be able to infect target systems to gain leverages. Those leverages can be different from simple data theft to system destruction. 30% of modern malware was capable of overriding signature- based intrusion detections. To overcome with this kind of intrusions, majority of organizations deploy endpoint detection and response (EDR) technologies [15].

Endpoint Detection and Response (EDR) is the process of monitoring and detecting, in real-time, any suspicious activity or events occurring at the endpoint [16]. This system provide real time alerts and details about the attack if any appears. With the use of advanced artificial intelligence threat agents, expected EDR tools able to learn and respond to the most advanced and undetectable malware attacks.

Many manufacturers in the security manufacturing space continue to invest in cloud-based solutions across their portfolios, anticipating continuing growth in demand for such products [17]. Moving on to cloud- based platforms became a trend in these days. Instead of using traditional IDS, centralized collaborative intrusion detection systems are proposed for better security for cloud infrastructure. This centralized intrusion detection systems collect and analyze the packets which come from different access points of the cloud system. Then the base station will send alerts if any positive intrusion occurs. Using this proposed method, the cloud system can detect black hole attacks and most forwarding attacks also this system gave energy efficiency and the increased performance for intrusion detection. Apart from that cloud environments more focus on host- based intrusion systems. Such systems basically trace intrusion by analyzing the system calls, which if any malicious activity performs using system calls can be detectable. This modal is categorized as, security as a service (SecaaS).

Recently research paper was released based on the deployment of a Stateful Protocol Analysis- based Detection System (SPADS) for IEC 60870-5-104 Supervisory Control and Data Acquisition (SCADA) networks. This proposed detection state machine uses IEC/104 traffic to detect and monitor intrusion on SCADA networks. Stateful protocol analysis is recommended by NIST to detect anomalous behaviors where SCADA protocols are used [20].

Machine Learning Ensemble Algorithms for IoT Malware Detection is another step forward. To improve the accuracy of botnet identification in Netflow data, two ensemble machine learning algorithms, Gradient Descent Classification (SGDC) and Ada-Boostand Stochastic. were used. The machine learning models are trained and tested using the CTU -13 benchmark dataset.

Cyber insurance is also an ongoing trend. Larger organizations to small businesses use cyber insurance services to increase their business liability against the intrusions. This services cover in addition to legal fees and expenditures, customers' personal identities are being restored and recovering data that has been tampered. Next generated firewalls (NGFW) also looking to deploy intrusion detection systems to their armory.

4. Conclusion

At present bulk amounts of malware and bots are creating to exploit more vulnerabilities on daily basis. With that ever- increasing threats and attacks, detection systems fail to provide 100% accurate results. Most of the malware undetectable in nature which means they sneak through all available defense mechanisms in the systems without leaving any footprints. It is a tough task to overcome such issues, sometimes intrusion detection systems provide false -positive alerts for bad packets which generated by corrupt DNS data, software bugs, or some other scaped data packets. With that increased false positive rate, most administrative persons ignore the intrusion alerts that might cause for entire system failure, if any real intrusion happens.

Nowadays, networks are in the Gigabyte speed range due to that it is too hard for intrusion detection systems to determine the normal traffic of the system. Apart from that lack of security datasets also downgrade the efficiency and accuracy of intrusion detection. It is mandatory to develop more compatible and accurate datasets to address more threats. Lack of infrastructure and user unawareness also jeopardized the system security. Hiring a subject awareness and experienced employees are obviously a better choice unless inside attacks cannot be inevitable.

It is always essential to develop an adaptive and fully automated intrusion detection system which has capable of adapting to any given circumstances. Sometimes IDS fails to produce expected outcomes in changing situations, deployment locations, environment configurations, and capacity of the computer resources name a few. Deploying such fully adaptive automated IDS gave efficient monitoring and analyzing capabilities with high accurate intrusion alerts.

5. References

[1] Onpassive “Artificial Intelligence in Cybersecurity” onpassive.com [Online]. Available: https://onpassive.com/blog/artificial-intelligence-in-cybersecurity/ [Accessed on 7 May 2021].

[2] Wikipedia “Hacker (disambiguation)” en.wikipedia.org [Online]. Available: https://en.wikipedia.org/wiki/Hacker [Accessed on 7 May 2021].

[3] Gil Press “A Very Short History of Artificial Intelligence AI” forbes.com [Online]. Available:https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/?sh=36bc2e4f6fba [Accessed on 7 May 2021].

[4] Rockwell Anyoha “The History of Artificial Intelligence” sitn.hms.harvard.edu [Online]. Available: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ [Accessed on 7 May 2021].

[5] S. Manandhar “Evolution of AI” lftechnology.com [Online]. Available: https://www.lftechnology.com/blog/ai/aievolution/#:~:text=In%20the%20past%20few%20years,in%20mobile%20and%20cloud%20platforms [Accessed on 11 May 2021].

[6] IBM Cloud Education “Deep Learning” ibm.com [Online]. Available: https://www.ibm.com/cloud/learn/deep-learning [Accessed on 11 May 2021].

[7] Scott "Esko" Brummel, MA[6] “Artificial Intelligence – Emerging Opportunities, Challenges, and Implications for Policy and Research (GAO Report)” scipol.duke.edu [Online]. Available: https://scipol.duke.edu/printpdf/content/gao-report-artificial-intelligence-%E2%80%93-emerging-opportunities-challenges-and-implications // [Accessed on 11 May 2021].

[8] THREAT STACK MARKETING TEAM “ The History of Intrusion Detection Systems (IDS) – Part 1” threatstack.com [Online]. Available: https://www.threatstack.com/blog/the-history-of-intrusion-detection-systems-ids-part-1 [Accessed on 11 May 2021].

[9] Guy Bruneau “The History and Evolution of Intrusion Detection” sans.org [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344 [Accessed on 11 May 2021].

[10]Techopedia “Creeper Virus” [Online]. techopedia.com Available: https://www.techopedia.com/definition/24180/creeper-virus [Accessed on 12 May 2021].

[11] Teresa F. Lunt, Ann Tamaru, Fred Gilham, R. Jagannathan, Caveh Jalali, Peter G. Neumann “A Real- Time Intrusion- Detection Expert System (IDES)” cerias.purdue.edu [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1666 [Accessed on 12 May 2021].

[12] The Editors of Encyclopaedia Britannica "Year 2000 bug, millennium bug" britannica.com [Online]. Available: https://www.britannica.com/technology/Y2K-bug [Accessed on 12 May 2021].

[13] V.Kanimozhi and T.Prem Jacob "Artificial Intelligence based Network Intrusion Detection with hyper-parameter opt imization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud Computing. " sciencedirect.com [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959518305976 // [Accessed on 13 May 2021].

[14] John Pirc "Detection/Prevention: Then, Now and the Future" secureworks.com [Online]. Available: https://www.secureworks.com/blog/the-evolution-of-intrusion-detection-prevention [Accessed on 13 May 2021].

[15] Travis Rosiek "What is a Next Generation Network Intrusion Detection System?" bluvector.io [Online]. Available: https://www.bluvector.io/next-generation-network-intrusion-detection-system/ [Accessed on 13 May 2021].

[16] Mark Stone "What is End Point Detection and Response? EDR security explain" cybersecurity.att.com [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/endpoint-detection-and-response-explained [Accessed on 13 May 2021].

[17] Vanderbilt Insights "The near future of Intrusion Detection : 4 trends to keep an eye on" www.ifsecglobal [Online]. Available: https://www.ifsecglobal.com/intruder-alarms-3/near-future-intrusion-detection-4-trends-keep-eye-on/ [Accessed on 14 May 2021].

[18] Sean Goldstein "The Future of Intrusion Detection" capsicumgroup.com [Online]. Available: https://capsicumgroup.com/the-future-of-intrusion-detection/ [Accessed on 14 May 2021].

[19] Ankita Bhutani and Preeti Wadhwani " Intrusion Detection System / Intrusion Prevention System (IDS / IPS) Market Size By Component" gminsights.com [Online]. Available: https://www.gminsights.com/toc/detail/intrusion-detection-prevention-system-ids-ips-market [Accessed on 14 May 2021].

[20] Yang, Y., McLaughlin K., Sezer S., Yuan Y. B. and Huang W. "Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security" pureadmin.qub.ac.uk [Online]. Available:https://pureadmin.qub.ac.uk/ws/portalfiles/portal/14448430/Stateful_Intrusion_Detection_for_IEC_60870_5_104_SCADA_Security.pdf [Accessed on 14 May 2021].