Data Science and Its Applications in Cyber Security

Dr. G. RoslineNesa Kumari[1], Dr. S. Satheesh Kumar[2], *Dr.V.K.Senthil Ragavan[3]
[1]Professor, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu-600073
[2]Associate Professor, Institute of Aeronautical Engineering, Dundigal, Telangana– 500043
[3]Professor, St. Martin's Engineering College, Secunderabad, Telangana – 500100
Email: vksenrag@yahoo.com

ABSTRACT

In a computing context, cyber security is undergoing massive shifts in technology and its operations in recent days, and data science is driving the change. To understand and analyse the actual phenomena with data, various scientific methods, machine learning techniques, processes, and systems are used, which is commonly known as data science. In this paper, I have briefly described the data science its evolution its application s in cloud security and how cyber security data science came in existence what kind of advantages are given by CSDS and its steps like, where the data is being gathered from relevant cyber security sources, and the analytics complement the latest data - driven patterns for providing more effective security solutions. The concept of cyber security data science allows making the computing process more actionable and intelligent as compared to traditional ones in the domain of cyber security. After that I have described the various upcoming challenges that can emerge after the frequent applications of cyber security data science(CSDS), how machine learning and deep learning are applicable in it and types of algorithms that can be applicable in it. So, the overall paper is not only focuses on the origins of Data Science but it also describes its modern uses for the relevant cyber security field and data driven intelligent decision making system can protect our system from known and unknown cyber attacks

Keywords: Data-Driven model, Cyber security data science (CSDS), Security Incident patterns, supervised learning, Cloud security.

1. Introduction

This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years. The following case of "On 15 January 2009, Conficker corrupted "Ultramar" the French Navy computer network. The service has then been quarantined, and flights at different airbases have been forced to land because they've not been able to update their flight schedules [1]. The United Kingdom Defense Ministry confirmed contamination of some of its key devices and computers. The virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield have confirmed infections to more than 800 machines. In a report on 2 February 2009, over a hundred of their machines were compromised by the Bundeswehr, the Federal Republic of Germany's united armed forces. In January 2010, the Information Network of the Greater Manchester Police triggered a pre-emptive disconnection of the Police Central Database for three days. Staff had to contact certain forces to carry out regular searches on cars and individuals [2]. Cyber incidents are particularly hazardous with Network Centric Warfare (NCW), and cyber defense alterations are urgently needed. The use of artificial intelligence techniques and knowledge-intensive tools would be vital in new offensive methods like dynamic installation of protected perimeters and integral crisis management, fully automated reactions to attacks in networks [3].

2. Research Methodology

To get an all-round impression of the junction between cyber security and AI, we used four databases: Scopus, Web of Science, ACM digital library also IEEE Explore. Along with that, we also used the Google Scholar search engine. A set of keywords matching the topics were searched for in these databases. To improve our search results and to make them more accurate, the authors refined various keywords from the search machine to obtain the maximum coverage [5].
In the additional step, obtained results were filtered. The search results which we got were limited only to the papers published in the last four years, as the determination of this paper is to bring out the newest trends of AI in cyber security. Last, the findings were categorized by the number of certifications. Besides those documents were selected, which had more than five citations. On the other side, newly published research papers that had less than five citations/references but innovative methods/approaches were also selected. The resources which meet the succeeding [6] requirements were subsequently accepted:

- Papers with titles belonging to subjects outside the scope of this research paper

- Technical Reports, Patent Documents, Books, Citations.
- Papers that had not been published in English

In the 3rd step, we inspected the conclusions besides the abstracts for filtering the pertinent information. This step helped the authors to find if the confidential papers coordinated the topic to find the junction between cyber security and AI. Accordingly, those papers were chosen which had the most relevant data and met our objective. The methodology followed was an extensive literature review to analyze the gaps. This study latches the gap by bringing together the effect of multiple areas, AI usage in the Security domain, methods implemented, and methods that were put forth. It is used to develop an overall architecture for future research in this specific domain [7].

3. AI in depth

As an area of study journal, artificial intelligence (AI) is about as ancient as computer systems (also called initial system intelligence). From the yesteryears of AI, it was "on the horizon" that devices/software/structures could be built cleverer than humans. The issue is that as time progresses, the time frame is going further. We saw a variety of machines, for example, playing really good chess, overcome sensibly complex problems [8]. The chess play was viewed during the initial periods of the computation as a test of intellectual ability. Although electronic chess was on the grandmaster during the seventies, a system that could defeat the global champion appeared almost difficult to develop. Yet quicker than anticipated, this happened. It has three reasons: improved computational power, design of powerful search algorithms. It could be utilized in several software beyond games like chess, see Check section below), and well-structured skill set which includes all possible chess information. The chess dilemma was basically solved as it was an abstract concern of the so-called small AI. Another example involves the translation of a particular AI from one dialect to the next [9]. In the 1960s, especially following N. Chomski 's research in computational linguistics, has been anticipated to address the issue of Natural Language Processing early. It hasn't yet occurred, even though certain unique programs such as Google's AI linguistics indicated initial success. This includes artificial intelligence gaining vast quantities of expertise in each aspect of human activities and obtaining the capacity to cope with it. AI can be regarded, in general, as an aspect of intellect, and broadly the creation of intelligent devices, as a technology that offers a solution to overcome difficult issues which cannot be solved without, for example, performing well or

creating correct choices due to large quantities of smartness [10]. In this article, we apply the right line, propose the application of particular AI methods in cyber defense issues and respond to the latest Artificial intelligence as illustrated in(*IOS Press*, n.d.).**4. The Role of AI in Cyber Security** Industries and private sector companies have already adopted AI programs, and as the White House notes, also many government departments utilize the tool. Why? Why? Since AI can easily save resources and time by scrolling through standardized data and comprehensively reading and studying unstructured data, numbers, speech patterns, and sentences. In fact, AI could save both tax dollars as well as national secrets. And there are gaps. Hackers are trying to figure out how to access the machines, slipping through cracks we didn't know were there. Years fly already then until a company finds a data leak [11]. By then, the hacker is long gone and all the sensitive data. On the other side, AI must sit back and collect data and wait until a hacker gets messy. AI checks for behavioral anomalies that hackers are expected to display for starters, whether a password is written, or when the user logs in. AI can detect those little signs that otherwise would have gone undetected and stop the hacking group in their routes. As Varughese noted, every device can be abused. Human hackers always will interrogate the weak spots in every system including AI in the constant cyber security chess game. Artificial intelligence is human-controlled and may still, therefore, be vanquished. Although AI is remarkable in its capacity to link and process data, it can only function as well as it was designed [12]. As hackers adjust to the Artificial Intelligence systems, new defensive measures will have to be deployed by the programmers. The game of cat and Industries and private sector companies have already adopted AI programs, and as the White House notes, also many government departments utilize the tool. Why? Why? Since AI can easily save resources and time by scrolling through standardized data and comprehensively reading and studying unstructured data, numbers, speech patterns, and sentences. In fact, AI could save both tax dollars as well as national secrets. And there are gaps. Hackers are trying to figure out how to access the machines, slipping through cracks we didn't know were there. Years fly already then until a company finds a data leak [11]. By then, the hacker is long gone and all the sensitive data. On the other side, AI must sit back and collect data and wait until a hacker gets messy. AI checks for behavioral anomalies that hackers are expected to display for starters, whether a password is written, or when the user logs in. AI can detect those little signs that otherwise would have gone undetected and stop the hacking group in their routes. As Varughese noted, every device can be abused. Human hackers always will interrogate the weak spots in every system including AI in the constant cyber security chess game. Artificial intelligence is human-controlled and may still, therefore, be vanquished. Although AI is remarkable in its capacity to link and process data, it can only function as well as it was designed [12]. As hackers adjust to the Artificial Intelligence systems, new defensive measures will have to be deployed by the programmers. The game of cat and mouse will proceed, but AI is a positive strengthening in the fight to secure data. Google introduced a graphical data learning model for Tensor Flow machine learning. 03.09.2019 search Implemented Neural Structured Learning (NSL), an open-source framework that uses the Neural Graph Learning technique to train data sets and data structures in neural nets.NSL works with the machine learning stage Tensor Flow and is designed to work for qualified besides incompetent machine learning professionals. NSL may render machine vision models, execute NLP, and run projections from interactive databases such as medical reports or graphs of information [13].

"The use of organized signals during training enables developers to deliver better predictive performance, particularly if the volume of data points is fairly limited," Tensor Flow engineers thought today in a blog post. "Structured-signal also exercises principals to more robust models. These methods have been widely used to improve the performance of the model in Google, such as learning semantic implanting of images [14]. NSL can work with monitored, semi-supervised, or unsupervised to construct representations that use graphic signals to regularize throughout development, with much less than ten code lines in certain instances. The original framework also contains tools that will help developer's structure data and APIs with little code for creating examples of vector quantization. In April, Google Cloud launched other organized data approaches, such as linked sheets in Big Query besides Auto ML Tables. In several other AI news, Google AI, formally known as Google Research, open-sourced SM3, a compiler for large-scale speech recognition models such as Google's BERT, too the GPT2 for Open AI [15].

AI is what brought us speech recognition apps (assume Siri), a search app from Google, and facial recognition tools from Face book. Many manufacturers of payment cards often use AI to aid investment banks in stopping trillions of dollars in recorded fraud. But what about the application of their Information Security?

Is artificial intelligence a benefit or a challenge to digital security in the business? On the one hand, modern information management infrastructure is valuable because it facilitates the evaluation, study, and understanding of cybercrime by safety practitioners. It strengthens the digital management strategies companies utilize to counter cybercrime and helping in keeping businesses and customers secure. Artificial intelligence, on the other hand, may be very resource-intensive [16]. That might not be possible in any implementation. In fact, it may also serve as a formidable armament in the computer offenders' arsenal that leverages technology to improve and intensify cyber-attacks.

The debate around artificial intelligence was nothing special in terms of information security. Information is, after all, at the very heart of cyber safety trends. But what better way to analyze the information than using computer systems that can think in nanoseconds and then perform tasks that would take people considerably longer?

AI is rapidly a field of emphasis inside the computer safety community. We will analyze advancements in security tools for AI and how the technology impacts institutions, cybercriminals, and consumers alike. Let's work it all out. Why automated information protection protocols better improve internet security? Whether you're like multiple increasing companies, you have a variety of security layers in place boundary, network, edge, device, and computer storage. [17] For e.g., you might have firewall rules for hardware or software in addition to network security systems that track besides determining which linked devices are authorized and avoid others. If hackers make these protections past, the antivirus and malicious solutions will be up to them. Then they could face IDS / IPS solutions, etc.

Yet what will happen as cybercrime overtakes certain protections? When the security of knowledge depends entirely on human-based surveillance capacities, then you are in trouble. After that, cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyber protection either. You need to be able to detect, identify and respond instantly to the threats 24/7/365. Irrespective of holidays, hours off work, even whether workers are simply unavailable, IT departments ought to be up to the job and ready to react promptly [18]. Artificial intelligence-powered information protection systems were designed to operate around the clock, shielding you. Infractions of a second, Artificial Intelligence may respond to cyber threats, which would require many minutes, hours, days, months, or even years to recognize by human beings.

5. Offerings that we have

After a review of the articles on AI technologies on cyber security, we may infer that there are already multiple important features in this field. Firstly, they are used in perimeter shooting neural networks. [28] On the other hand, it is obviously only because AI approaches were used that even more cyber security problems could be overcome efficiently. In decision making, comprehensive information use is needed, and sound decision assistance is one of the cyber security's unresolved problems. In the artificially intelligent sector, a broad variety of approaches has been established for the resolution of complicated situations, which involve human intelligence [24]. Most of these strategies have attained a mature phase where specific algorithms based on these approaches are available. Several methods are even so prominent that they are no longer considered as a part of artificial intelligence. They are now a part of certain applications, such as data mining algorithms, which emerge from AI's learning subfield. In a short survey, you will not be able to attempt to include a more or less comprehensive overview of all practicable AI approaches. We have also divided approaches and architectures into multiple categories: artificial neural, expert systems, smart agents, quest, computer education, data gathering, and constraint resolution. Here we define the following groups and refer to the use of respective cyber protection approaches. We do not cover machine vision, robotics, and comprehension of natural languages that we find in particular AI applications. Robots and machine views undoubtedly have amazing military capabilities, but nothing unique to cyber security has been observed there [25].

5.1 Neural Nets

Network Neural has had a long background starting with Frank Rosenblatt's discovery of the perception in 1957 an artificial neural network that is one of the most common neural network components. Already a limited combination of perceptions will study and resolve fascinating issues. Yet, a huge proportion of neural networks could be made of neural networks. Neural networks thus include a parallel distributed learning and decision-making capability [26]. The operating frequency is their most defining characteristic. These are ideal for identification of learning patterns, grouping, a compilation of threat responses, ((4) Use of Artificial Intelligence Techniques / Applications in Cyber Defence, n.d.), etc. They may be applied in applications or electronics. Intrusion detection techniques avoidance is also applicable to neural networks. Plans were created in DoS detection, software worm identification, spam filtering, zombie identification, analysis of malware, and forensic science.

The fast mobility, whether implemented in hardware or used in graphical chipsets, causes the prominence of deep learning in computer security. The innovation of neural nets is new: cognitive nets of third-generation – rocketing machine learning that more effectively imitate artificial neurons and which offer greater possibilities for application. The use of FPGAs (field gate arrays) is a great way to rapidly build and adapt neural networks to changes in risks. They provide interesting possibilities.

5.2 Expert Systems

The most commonly deployed AI methods are certainly specialist programs. An expert program is a technology to seek solutions to problems raised either by a customer or a certain technology in a certain technology area. This may be used specifically in decision-making assistance, for example, with medical care, banking, or virtual worlds. There are various optimization techniques for solving complicated problems size from tiny analytical medical diagnoses to highly advanced hybrid systems. A scheme of expertise comprises a knowledge base that contains the specialist analysis of a specific application area [27]. In advisement to the knowledge base, this contains a deduction engine that offers solutions based on that understanding. Vacant understanding and motor of implication are commonly referred to as a current plastic understanding must be filled before it is used. The artificial intelligence shell must be endorsed by knowledge base software and can be lengthened by interactive query

programs and with other programs which can be used in skilled hybrid engines. The advancement of a specialist system means, first, that the artificial intelligence shell should be selected and adapted, and, second, that erudite knowledge is gathered and the learning's supplied. The second step is far longer and much more complex than the first step. The development of intelligent machines has many hours, days, months, or even years to recognize by human beings. methods. In general, a device contains an artificial intelligence shell and has usability to add understanding to the repository of information.

There are several types of representations in expert systems, and the most general is stabilizers interpretation. Artificial intelligence may provide additional functionalities for simulation and so on, etc. Nevertheless, the importance of a master system primarily relies on the consistency of data in the skill set of the master system and not so much on the on-premises nature of the delineation of expertise. For security preparation, the instance of a cyber security device specialist is one. This skilled system enables substantially the collection and instruction of security initiatives to optimize the use of scarce resources. Initial stuff on the deployment of professional detection techniques is underway.

5.3 Intelligent Agents

Computational intelligence software components with some smart-action features which make themselves special: proactive, ACL, reactive (capabilities to make and act certain decisions). Intelligent agents are software applications. They may have the capacity to prepare, organize and evaluate. There is indeed a notion of software agents in the software development community in which they are seen as artifacts that at least proactively use the networking language of an agent. Differentiating agents and subjects, subjects can be passive and have no communication to comprehend (though they embrace strictly delineated syntax messages).

Intelligent agents were used to protecting DDoS, and simulations were described where it is possible to effectively protect cooperation agents from the attacks of DDoS. When all regulatory and contractual problems have been addressed, a 'cyber police force' composed of mobile smart officers would, in practice, be feasible. This would include technology to enable mobility and connectivity of cyber personnel, which must be inaccessible to opponents. Cooperation with ISPs is important. However, if further experience can be used to direct the search, it can greatly enhance the efficacy of the quest. Almost every smart system has some type of quest, and its quality is often important for its overall performance.

5.4 Search

A broad variety of search techniques is created that takes detailed focus on specific search problems into consideration. Although numerous search techniques in AI were established and are commonly used in many applications, they are rarely used as using AI. Of one, the search is embedded in the application stack and is not seen as an AI function. In this sense, dynamic analysis programming is used primarily to address optimal security concerns. Check on besides- or trees, αβ-index, minimal check-in addition stochastic index is commonly used in the applications of gamers and is useful in network security decision-making. Originally designed for software chess, the αβ-search algorithm is an adaptation of a common assistance principle "divide and conquer" in the resolution of problems and, in particular, in decisions where two opponents chose their absolute best move. This uses minimum expected gain and cumulative potential loss figures. Perhaps you can disregard a vast range of options and speed up the quest considerably.

5.5 Learning

Learning strengthens the information structure through the extension, reorganization, or enhancement of the knowledge base. It is one of the most important artificial intelligence topics being studied intensively. Calculative approaches for gaining new ideas, new abilities, and innovative ways to coordinate current knowledge require computer learning. Learning challenges range widely from basic parametric learning, which means knowing the meaning of

such quantities, to complex types of abstract teaching, such as concept learning, grammar learning, usability, and behavioral teaching.
AI offers both monitored (learning with a teacher) and unattended learning forms. The above is particularly helpful where vast volumes of data are present. In addition, this is popular in cyber security, where massive logs can be obtained. Initially, data mining was derived from uncontrolled AI learning. Uncontrolled learning may be a function of self-organized neural networks, in general. Parallel neural networks are used for output in parallel hardware with a distinctive class in learning techniques. These methodologies of learning are defined by an evolutionary algorithm and neural networks. For instance, genetic analytics, in addition to fuzzy logic, was used in mentioned threat detection methods.

6. Challenges

When you intend future study, production, and implementation of AI approach on cyber security, you will differentiate among imminent targets and long-term outlooks. Multiple AI approaches can be used on cyber security quickly, and urgent cyber security challenges need smarter solutions than they are actually applied. So far, these current immediate apps have been mentioned. The introduction of entirely new concepts of information processing in the management of circumstances and decision-making in the future would be exciting. Knowledge management for net central warfare is a demanding technology field. The rapid evaluation of the situation, which allows leaders and policymakers dominance at every point, is achieved only by automatic information management. The review gives an overview of the centralized and decentralized information model in the Bundeswehr modern command and control structure. Having a potential horizon in mind maybe we should not only rely on the Narrow AI for at least a couple of decades to come Some people are tempted that the AI's main goal – artificial cognition creation AGI can be accomplished in the mid-20th century. In 2008 the first AGI meeting took place at Memphis University. Founded in 2000, the Singularity Institute for Artificial Intelligence (SIAI) alerts investigators that there could be the risk of increasingly accelerated intelligence growth on machines. This can progress to Singularity, defined as follows: "Singularity is the technical advancement of intellect that is smarter than an individual. There are many developments that are commonly listed as a path forward. The most frequently discussed is currently Artificial Intelligence, but many other developments enable the development of intelligent intelligence, provided they meet a threshold degree of complexity.

7. Conclusion

In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cyber security strategies cannot be ignored. Also, security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smart approaches are used. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cyber security. Neural network implementations continue on cyber security. For many fields where neural networks weren't the most appropriate technologies, sophisticated cyber-security approaches are still desperately needed. Such fields include decision support, understanding of the situation, and control of information. The most interesting in this scenario is expert machine development.
Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that the perpetrators will exploit a new form of artificial intelligence as long as it is accessible. This is not obvious. In addition, the latest technology in the understanding, interpretation, and management of information, particularly in the area of computer learning, would significantly improve systems' cyber security capabilities.

References

[1] *Use of Artificial Intelligence Techniques / Applications in Cyber Defense*. (n.d.). Retrieved 14 August, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense.

[2] Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. *SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks*, 229–234. https://doi.org/10.1145/1626195.1626252.

[3] Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3973 LNCS*, 255–260. https://doi.org/10.1007/11760191_37.

[4] Bitter, C., North, J., Elizondo, D. A., & Watson, T. (2012). An introduction to the use of neural networks for network intrusion detection. *Studies in Computational Intelligence*, *394*, 5–24. https://doi.org/10.1007/978-3-642-25237-2_2.

[5] Carrillo, F. A. G. (2012). ¿Can Technology Replace the Teacher in the Pedagogical Relationship with the Student? *Procedia - Social and Behavioral Sciences*, *46*, 5646–5655. https://doi.org/10.1016/j.sbspro.2012.06.490.

[6] Chang, R. I., Lai, L. Bin, & Kouh, J. S. (2009). Detecting network intrusions using signal processing with query-based sampling Filter. *Eurasip Journal on Advances in Signal Processing*, *2009*. https://doi.org/10.1155/2009/735283.

[7] Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A Distributed Intrusion Detection Prototype using Security Agents. *HP OpenView University Association*, *June 2014*.

[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6070 LNAI*(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19.

[9] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). *Innovations in Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07)*. *44/2008*(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10] Feyereisl, J., & Aickelin, U. (2009). *S Elf -O Rganising M Aps*. *August*, 1–30.

[11] Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1907*, 93–109. https://doi.org/10.1007/3-540-39945-3_7.

[12] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. *IEEE Transactions on Fuzzy Systems*, *20*(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

[13] *IOS Press*. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithms-and-architectures-of-artificial-intelligence/.

[14] Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4476 LNAI*, 212–228. https://doi.org/10.1007/978-3-540-72839-9_18.

[15] Kotenko, I. V, Konovalov, A., & Shorov, A. (2010). Agend-based Modeling and Simulation of Botnets and Botnet Defense. In *Conference on Cyber Conflict* (pp. 21–44). http://ccdcoe.org/229.html.

[16] Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. *MODELSWARD 2013 - Proceedings of the 1st International Conference on Model- Driven Engineering and Software Development*, 312–315. https://doi.org/10.5220/0004348203120315.

[17] Pachghare, V. K., Kulkarni, P., & Nikam, D. M. (2009). Intrusion detection system using self organizing maps. *2009 International Conference on Intelligent Agent and Multi-Agent Systems, IAMA 2009*, *4*(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074.

[18] Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering*, *5*(12), 317–322.