SanskritiManthan : International Journal of Empowerment & Indian Culture
संस्कृतिमंथन: सशक्तीकरण आणि भारतीय संस्कृतीवरील आंतरराष्ट्रीय संशोधन पत्रिका
संशोधनातून संस्कृतीचा साक्षात्कार

The Role of Machine Learning and AI in Modern Cyber Security

Mr.Yogesh Devidas Patil
mPHATEK Systems Pvt Ltd
Jr.Software Developer
Yogeshpatil9551@gmail.com
7721923650

Abstract

Managing the difficulty of operations and the huge amount of information required to protected cyberspace is beyond human capacity without significant automation. However, conventional fixed-logic software systems face limitations when addressing modern security threats. To overcome these challenges, AI-driven techniques like machine learning offer promising solutions. This paper presents an overview of the various AI applications in cybersecurity and evaluates the potential for strengthening defense mechanisms using these technologies. The analysis of current AI-based cybersecurity tools reveals that neural networks, in particular, are already providing protection in areas such as perimeter security and other domains. However, some cybersecurity challenges, especially those related to strategic decision-making, require AI-powered approaches to be fully addressed. Effective decision support, driven by comprehensive data analysis, remains one of the critical unresolved issues in cybersecurity.

Keywords: Artificial Intelligence, Intelligent Agents, Neural Networks, Advanced Cybersecurity Techniques

1. Introduction:

It has become increasingly evident that only advanced technologies can effectively defend against the growing complexity of cyber threats, as the sophistication of cyber-attacks & malware has escalated rapidly over the past few years. A notable example is the Conficker worm attack on 15 January 2009, which infected the French Navy's "Ultramar" computer network. As a result, the network was isolated, & flights at various airbases were grounded since they were not able to update flight schedules [1]. Additionally, the UK Ministry of Defence reported that several key systems and computers were compromised. The virus spread through various government sectors, including hospitals & Navy Star/N* desk departments in Sheffield confirmed that above 800 of their machines were infected. Similarly, a report on 2 February 2009 revealed that more than a hundred devices within the Bundeswehr, Germany's unified armed forces, were affected. In January of 2010, the Greater Manchester Police Information Network was forced to disconnect the central police database for three days as a precaution, requiring staff to rely on manual contact with other forces for routine checks on vehicles and individuals [2].

Cyber incidents pose a significant threat, particularly in the context of Network Centric Warfare (NCW), highlighting the urgent need for improved cyber defense strategies. Employing artificial intelligence will be critical in developing new invasive and defensive approaches, such as dynamically securing perimeters, managing crises comprehensively, and automating responses to network attacks [3].

The role of intelligent applications in cyber war has seen a dramatic surge. A close examination of the cyber domain provides insight into this trend. One key reason is that artificial intelligence enables rapid responses to evolving online threats. Managing huge amounts of data in real time is essential for understanding and interpreting cyber activities, as well as making informed decisions. Without advanced technology, humans would struggle to keep pace with both the speed of cyber operations and the sheer volume of data involved. Traditional machines, relying on fixed algorithms with pre-programmed decision-making logic, are insufficient for defending against ever-evolving cyber threats. This creates an opportunity for the use of AI-driven automated technologies [4].

Later sections of this paper will explore various fields of science & technology that leverage artificial

intelligence. In Chapter 3, we will examine existing AI implementations in cybersecurity, categorized by their respective AI methodologies. Chapter 4 will discuss future opportunities, introducing innovative smart tools and technologies for cyber defense.

2. Research Methodology:

To gain a comprehensive understanding of the intersection between artificial intelligence & cyber security, we utilized four primary databases: **Web of Science, Scopus, IEEE and ACM Digital Library Xplore**, supplemented by the use of **Google Scholar**. A set of targeted keywords relevant to the research topic was employed to conduct searches across these platforms. In order to increase the accuracy and coverage of the search results, we refined the keywords iteratively during the search process to ensure broad yet relevant findings [5].

The next step involved filtering the initial results. We restricted our search to publications from the past few years, as the objective of this research is to highlight the most current trends in AI applications within cyber security. In addition, we categorized the findings based on the number of citations. Papers with at least five citations were prioritized, though recently published papers with fewer citations but innovative approaches were also considered. The following criteria were applied to select the most suitable resources [6]:

- Papers with titles that were not aligned with the focus of this study.
- Technical reports, patents, books, and citations.
- Papers those not published in English.

In the third stage, we thoroughly reviewed the abstracts and conclusions of the selected papers to extract relevant information. This process allowed us to identify papers that specifically aligned with the intersection of cybersecurity and AI, ensuring the data met the research objectives. The methodology used involved a thorough literature review to identify gaps in current research. This study addresses these gaps by consolidating insights from multiple areas, including AI applications in cybersecurity, the methods implemented, and potential future approaches. The findings are aimed at building a conceptual framework for further research in this area [7].

3. AI in Depth:

As a field of research, artificial intelligence is nearly as old as computer systems themselves, often referred to as early system intellect. From the inception of AI, there has been an ongoing belief that machines, software, or systems could one day surpass human intelligence. However, as time has passed, this goal seems to remain perpetually in the future. Nevertheless, we've witnessed machines capable of performing tasks like playing chess at an impressive level and solving reasonably difficult problems [8].

In the initial days of computing, chess was considered a key test of intellectual capability. While machines could compete at the grandmaster level by the 1970s, it looked closely difficult to create a system that could defeat the world winner. Yet, this milestone was achieved sooner than estimated due to three primary factors: the rise in computational power, the development of sophisticated search algorithms (which have since been applied to many areas beyond games like chess), and the creation of well-structured knowledge bases that contained comprehensive information about chess. Essentially, the chess problem, as a theoretical challenge in the realm of "narrow AI," was solved. Another notable example of AI's progress is its ability to translate languages, a capability that began to develop in the 1960s [9].

Inspired by Noam Chomsky's pioneering work in computational linguistics, researchers had high hopes that Natural Language Processing (NLP) would be tackled early on. However, despite early successes with specialized programs like Google’s AI-driven linguistic tools, a comprehensive solution has yet to be fully realized. AI’s advancement involves accumulating extensive knowledge across different areas of developing the ability and human activity to manage and process this information effectively. In a broader sense, AI is a representation of intelligence and the development of smart systems, offering solutions to complex problems that are otherwise unsolvable—such as optimizing performance or making accurate

decisions when dealing with vast amounts of information [10].

This article follows a strategic approach by proposing the use of specific AI techniques to address challenges in cybersecurity and highlights the latest advancements in AI, as discussed in publications like IOS Press (n.d.).

4. Role of Artificial Intelligence in Cyber security

4.1 Is AI playing vital role to the Future of Cyber security?

AI has already been widely embraced by industries and private companies, and as highlighted by the White House, numerous government agencies are too utilizing AI. The reason for this adoption is clear: AI saves both resources & time by efficiently processing structured data and analyzing vast amounts of speech patterns, unstructured data, including numbers & text. In fact, AI has the knowledge to safeguard national security and reduce costs for taxpayers. However, vulnerabilities still exist. Hackers continually search for ways to exploit weaknesses, finding gaps in systems that often go unnoticed for years, allowing sensitive data to be compromised long before the breach is detected [11].

AI, however, can take a more proactive stance by monitoring data and waiting for hackers to make mistakes. It can identify behavioral anomalies that hackers may display, such as unusual login times or inconsistencies in password usage. By spotting these subtle clues, AI can thwart cybercriminals before they can cause serious harm. As Varughese pointed out, every system, including those powered by AI, can be exploited. Human hackers will always attempt to find vulnerabilities, even in AI, in the never-ending cybersecurity battle. While AI is impressive in its ability to process and connect data, it is only as strong as its programming allows [12].

As hackers evolve to counter AI systems, developers will need to deploy new defense mechanisms to keep up. Although the mouse-and-cat game will continue, AI remains a powerful tool in securing data. For example, Google has presented a machine learning framework called TensorFlow, designed to facilitate graphical data learning. On September 3, 2019, Google released Neural Structured Learning (NSL), an open-source framework that uses Neural Graph Learning to train datasets and structures within neural networks. NSL is integrated with TensorFlow and designed to be friendly to both experienced and novice machine learning practitioners. The framework can improve machine vision models, run natural language processing (NLP), and predict using data from interactive sources, like medical records and knowledge graphs [13].

In a blog post, the engineers at TensorFlow explained that "structured signals during training enable developers to" improve predictive accuracy, particularly when data points are limited." They also added that structured signals contribute to creating stronger models, which has been proved by Google applying these techniques to image embedding models in tasks such as semantic understanding [14]. NSL supports supervised, semi-supervised and unsupervised learning, This enables developers to construct models utilizing graph-based signals with a small amount of lines of code. Additionally, the framework supports data structuring and generation examples with vector quantization in APIs. In the month of April, Google Cloud announced other structured data approaches, such as connected sheets in AutoML Tables & BigQuery. Additionally, Google AI released SM3, an optimizer designed for large scale machine learning models, including those used in speech recognition, such as Google's BERT and OpenAI's GPT-2 [15].

AI has revolutionized the way we interact with technology, powering applications like voice recognition, Facebook’s facial recognition tools and Google’s search engine. Several payment card providers also rely on AI to help investment banks in detecting and preventing billions of dollars' worth of fraud. But what role does AI play in information security?

Is artificial intelligence a valuable asset or a potential challenge for business cybersecurity? On one hand, modern AI-driven information management systems help security professionals analyze, understand, and combat cybercrime more effectively. AI strengthens digital security strategies that businesses use to protect themselves and their customers. Conversely, AI can be resource intensive, potentially making it impractical in

some applications [16]. Additionally, AI might become a double-edged sword, as cybercriminals can also harness its power to launch more sophisticated and destructive cyberattacks.

The role of AI in cybersecurity is not a new topic. Information is central to cybersecurity, and AI offers unparalleled speed in processing and analyzing large amounts of data, making it ideal for identifying threats that would take humans far longer to detect and respond to. As a result, AI has become a major focus in the cybersecurity community, with discussions centered on how AI-powered security tools can impact organizations, cybercriminals, and consumers alike.

Why do automated security protocols enhance online protection? If your business is like many others, you have multiple layers of security—network, edge, device, and data storage—to protect against threats [17]. For instance, you might have firewalls in place, along with security systems that monitor and authenticate devices. Should a hacker break these defenses, malware and antivirus detection solutions are the next line of protection, followed by intrusion prevention systems (IPS) and intrusion detection systems (IDS).

But what happens when cybercriminals outsmart these defenses? If your organization relies solely on human-driven surveillance and response capabilities, you are at a significant disadvantage. Cybercrime doesn't follow a predictable schedule, and your vulnerabilities don't take breaks either. To effectively combat threats, organizations need to notice, analyze, and reply to attacks 24/7, regardless of holidays, staff availability, or work hours. This is where AI-driven cybersecurity systems shine. AI can respond to cyber threats in milliseconds—something that could take humans minutes, hours, or even longer to detect.

4.2 What Do AI Leaders Think About AI in Cybersecurity?

A research by the Research Institute of Capgemini titled *"Reinventing Cybersecurity with AI"* underscores the growing significance impact of AI in cyber security defences. The study surveyed 850 cybersecurity, IT, and data management leaders across 10 countries, and found that AI is becoming indispensable as cybercriminals themselves are starting to use AI to carry out attacks. Some key findings include: 75% of respondents agreed that AI allows their organizations to reply to breaches more quickly, and 69% stated that AI is essential for staying ahead of cyber threats [19]. Furthermore, 60% of firms reported that AI makes cybersecurity analysts more accurate and efficient.

As networks grow more complex and expansive, AI is likely to play a vital role in bolstering enterprise cyber security defenses. The sophistication of modern networks has exceeded the capabilities of human operators alone, making AI an indispensable tool. However, the question remains: what steps should businesses take to ensure that their confidential data and customer information remain secure?

4.3 Integrating Artificial Intelligence into Your Cybersecurity Strategy

Incorporating artificial intelligence (AI) into existing cybersecurity frameworks is not something that can be done instantly. It requires thoughtful planning, training, and preparation to ensure that both the systems and the teams controlling them can use AI properly. By Naveen Joshi, CEO of Allerin, points out in a Forbes article that There are many ways AI can enhance the sustainability. and efficiency of cybersecurity activities, including::

- Implementing biometric-based password systems for more secure login processes
- Using predictive analytics to detect potential threats and suspicious activities
- Enhancing decision-making and data analysis through natural language processing (NLP)
- Securing identity and network connections by setting strict access controls

Once AI is integrated into your information security systems, your cybersecurity professionals and IT staff will need time to understand how to utilize these tools effectively. Training and planning are made to ensure Maximizes the benefits of AI in your organization integration. It's easy to forget not to ignore the human element—the investment in training employees. Awareness is essential.

Some of the big names in the industry already are embracing AI for cybersecurity. Such major players include Palo Alto Networks, Fortinet, Check Point, LogRhythm, Sophos, CrowdStrike, Symantec, and FireEye. Despite these benefits, there are challenges as well. The primary problem of AI in cybersecurity is the higher cost and longer time required to implement than that of traditional, non-AI-based security solutions. The most expensive tools are AI-driven cybersecurity, and thus, small and medium-sized businesses can hardly afford them.

Newer SaaS models are arising that make AI-powered cyber security solutions available to a wider group of companies at lower prices. It's frequently more economical to invest in AI-driven security measures rather than to suffer through the impact of cyber-attacks, such as fines, delays, and other costs.

4.4 Addressing Vulnerabilities Introduced by AI Cybersecurity Tools

While AI is of much importance for malware and cyber threats detection and combat, it also poses new challenges. Cyber attackers can make use of AI technologies to stage even more advanced attacks. As the cost for designing and implementing AI technologies reduces, classy machine learning tools are rendered accessible to cyber criminals. It offers more possibilities of exploitation to the attackers.

4.5 Adversarial AI: How Cybercriminals Can Exploit AI

Misuse of AI in cybersecurity is referred to as "adversarial AI." Adversarial AI refers to the misuse of AI for malicious purposes where attackers manipulate machine learning algorithms to misconstrue inputs and behave in ways that benefit the intruder. In essence, adversarial AI tricks neural networks into misclassifying or misrepresenting data through altered inputs.

Without proper defenses, AI may expose organizations to high risks. Fortunately, there are cybersecurity specialists who are fully aware of these threats and are working in earnest to counter them. Indeed, as the article from the IBM's Security Intelligence blog points out, white-hat hackers are developing defenses while testing AI systems for their vulnerabilities. IBM's Dublin lab, for instance, has created the Adversarial Robustness Toolbox (ART), a toolkit designed to improve the resilience of AI systems against adversarial attacks.

5. Offerings Overview

A review of articles discussing AI technologies in the realm of cybersecurity reveals several significant features. Notably, these technologies are employed in perimeter defense utilizing neural networks. The effectiveness of AI methodologies has enabled the well-organized resolution of various cybersecurity challenges. Information utilization is essential for effective decision-making, and enhancing decision support remains a key unresolved issue in cybersecurity. The arena of artificial intelligence has developed a various array of strategies to address complex problems, often mimicking human cognitive processes. Many of these approaches have matured to the topic where exact algorithms derived from them are widely available. Some methods have become so established that they are no longer seen purely as AI techniques; instead, they are integrated into applications like data mining algorithms that stem from AI’s machine learning sector.

In this brief overview, we do not aim to present an exhaustive account of all viable AI approaches. Instead, we categorize the strategies and architectures into several groups, including artificial neural networks, expert systems, intelligent agents, query systems, constraint resolution , data gathering, and computer education. Notably, we exclude areas such as machine vision, robotics, and natural language processing, which are prominent in specific AI applications. While robotics and machine vision offer remarkable capabilities, they do not present unique contributions to cybersecurity.

5.1 Neural Networks

Neural networks have a rich history, tracing back to Frank Rosenblatt's invention of the perceptron in 1957, which is one of the foundational components of artificial neural networks. Even a simple combination of perceptrons can tackle intriguing problems. However, the potential for creating complex neural networks is

vast. These networks have parallel distributed learning and decision-making capabilities, enabling them to identify learning patterns, cluster, and build threat responses. They apply in electronics and intrusion detection, where they mitigate threats. Applications of neural networks include DoS attacks, software worms identification, spam filtering, zombie detection, forensic investigations, and malware analysis. Their rapid processing powers either on hardware or in the graphic chipsets make them an essential feature of machine learning. Inventions in terms of third generation cognition, in cognitive networks rev up machine learning processes because a closer simulation of an artificial neuron can be realized. With the usage of Field Programmable Gate Arrays FPGAs neural networks may more effectively and speedily become tailored according to developing malicious acts.

5.2 Expert Systems

Expert systems are among the most widely utilized AI methodologies. These systems are designed to find solutions to specific problems presented by users or particular technologies within a defined domain. They are especially valuable for decision-making support in areas such as healthcare, finance, and virtual environments. Various optimization techniques exist for tackling complex challenges, ranging from simple medical diagnoses to sophisticated hybrid systems. An expert system typically integrates a knowledge base that encapsulates some specialized insights within the particular application area. These kinds of knowledge bases should always be complemented with some deduction engine that finds out solutions based on the kind of information available. At least before its application, the engine requires a sound knowledge base, which at times has to be brought out through continuous learning. The development of an expert system includes choosing and tailoring an AI framework along with gathering and integrating knowledge from the expert into the system. In most cases, this is more time-consuming and complicated than the above phase. Creating intelligent machines involves various approaches, and in general, these machines are made up of an AI framework capable of augmenting the knowledge base.

Expert systems use many forms of representation, but the most common is rule-based interpretation. AI can add more functionalities to these systems, including simulation capabilities. Ultimately, the effectiveness of an expert system depends more on the quality of the data within its knowledge base than on the specifics of its design. A more relevant example in the cybersecurity domain would be an expert system aimed at optimizing the management of security initiatives to make optimal use of the available scarce resources. Efforts have already been made towards professionalization of the methodology in this framework.

5.3 Software Agents

Software agents are the developed parts of intelligent agents which possess superior capabilities to set them apart as proactive, adaptive, and reactive entities which make and carry out decisions. These software applications possess planning, organizing, and assessment functions for tasks. The term "software agents" is used to describe artifacts in the domain of software development which actively engage in using the agent's networking language. Unlike subjects, which are passive and can neither express nor understand anything beyond a strictly defined syntax, intelligent agents are active participants.

These agents have been utilized for protecting against Distributed Denial-of-Service attacks and the simulations have indicated that these agents are good enough for protecting cooperative agents against such threats. Once all regulatory and contractual considerations are addressed, the establishment of a 'cyber police force' made up of mobile intelligent officers could become a reality. This would necessitate technologies that ensure the mobility and connectivity of cybersecurity personnel while remaining impervious to adversaries. Collaboration with Internet Service Providers (ISPs) is crucial for success. Moreover, leveraging past experiences to guide searches can significantly enhance the effectiveness of these systems. Most intelligent systems incorporate some form of search function, which plays a vital role in their overall performance.

5.4 Search Techniques

A wide range of search methodologies has been developed, focusing on particular search challenges. Although numerous search techniques in AI have been created and are widely applied, they are seldom recognized explicitly as AI functions. Instead, search functionalities are often embedded within the application layer. For instance, dynamic analysis programming primarily addresses optimal security issues. Techniques like tree searches, αβ-indexing, minimal checking, and stochastic indexing are commonly utilized in gaming applications and play a significant role in network security decision-making. The αβ-search algorithm, originally devised for software chess, exemplifies a common "divide and conquer" strategy for problem-solving, particularly in scenarios where two adversaries make optimal moves. By utilizing expected minimum gains and potential cumulative losses, this method allows for the efficient elimination of numerous options, thus accelerating the search process.

5.5 Learning

Learning is a critical component of artificial intelligence, focusing on enhancing the knowledge structure through the addition, reorganization, or refinement of information. It is one of the most extensively researched topics in the field of AI. Various computational methods are employed to acquire new insights, develop new skills, and innovate ways to integrate existing knowledge. Learning challenges can range from fundamental parametric learning understanding the significance of specific variables to more complex forms of abstract education, including concept acquisition, behavioural teaching, usability and grammar learning.

AI encompasses both unsupervised and supervised learning approaches. The latter is especially beneficial when dealing with large datasets, which is common in cybersecurity due to the availability of extensive log files. Initially, data mining techniques were developed from unsupervised AI learning. This type of learning can often be attributed to self-organizing neural networks. Parallel neural networks are utilized to produce outputs in parallel hardware and represent a unique category of learning techniques. These learning methodologies are characterized by the integration of evolutionary algorithms and neural networks. For example, threat detection methods have incorporated genetic algorithms alongside fuzzy logic.

6. Challenges

When considering future development, research, and implementation of AI techniques in cybersecurity, it is crucial to differentiate between long term aspirations and immediate goals. Various AI methodologies can be promptly applied to address cybersecurity issues, yet pressing challenges demand more sophisticated solutions than those currently in use. The existing applications have been discussed, but the prospect of introducing entirely new paradigms for information processing in situational management and decision-making is particularly intriguing. The field of knowledge management for network-centric warfare presents significant technological challenges. Effective automatic information management is essential for rapid situational assessment, enabling leaders and policymakers to maintain control in any scenario. This review highlights the decentralized & centralized information models utilized within the Bundeswehr's modern command and control framework.

As we look toward the future, it's important to recognize that we may not be able to rely solely on narrow AI for the next few decades. Some believe that achieving the ultimate goal of AI—creating artificial general intelligence (AGI)—could be possible by the mid-21st century. The first AGI conference occurred at Memphis University in 2008, and the Singularity Institute for Artificial Intelligence (SIAI), established in 2000, warns researchers about the potential risks associated with rapidly advancing machine intelligence. This phenomenon, referred to as the Singularity, is characterized by the development of intelligence that surpasses human capability. Many advancements are often discussed as pathways to this goal, with artificial intelligence being the most frequently cited. However, numerous other developments may also contribute to the emergence of intelligent systems, provided they achieve a sufficient level of complexity.

7. Conclusion

As malicious intelligence and cyber threats grow at an alarming rate, the importance of advanced cybersecurity

strategies cannot be overlooked. Experience in preventing Distributed Denial-of-Service (DDoS) attacks has shown that effective countermeasures can be implemented even with limited resources when intelligent strategies are employed. Literature reviews indicate that study on artificial neural networks offers the most relevant insights from AI applicable to cybersecurity. The deployment of neural networks in cybersecurity continues to evolve, yet there remains a pressing need for advanced security solutions in areas where neural networks may not be the most appropriate technology. These areas include decision-making support, situational awareness, and information control, with a particular focus on the development of expert systems.

The speed at which general artificial intelligence is advancing remains uncertain, but there is a risk that malicious actors could leverage new forms of AI as they become available. This potential threat is not to be taken lightly. Furthermore, advancements in the understanding, interpretation, and management of information—especially in the realm of machine learning—could greatly enhance the cybersecurity capabilities of systems.

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/algorithmsand-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 ModelDriven 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. https://doi.org/10.26438/ijcse/v5i12.317322.

[19] Protect yourself from the Conficker computer worm. (2009). Microsoft. http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.

[20] REFERENCES 1 2 R A Poell P C Szklrz R3 Getting | Course Hero. (n.d.). Retrieved 14 August, 2020,fromhttps://www.coursehero.com/file/p40hov9n/R-EFERENCES-1- httpenwikipediaorgwikiConficker-2-R-A-Poell-P-C-Szklrz-R3-Getting/.

[21] Rajani, P., Adike, S., & Abhishek, S. G. K. (2020). ARTIFICIAL INTELLIGENCE : THE NEW AGE. 8(2), 1398–1403.

[22] Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461). https://doi.org/85-460-1.

[23] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/ijerat.2020.3612.

[24] Shankarapani, M. K., Ramamoorthy, S., Movva, R. S., & Mukkamala, S. (2011). Malware detection using assembly and API call sequences. Journal in Computer Virology, 7(2), 107– 119. https://doi.org/10.1007/s11416-010-0141-5.

[25] Tyugu, E. (2011). Artificial intelligence in cyber defense. 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 95–105.

[26] Venkatesh, G. K., Nadarajan, R. A., Venkatesh, G. K., Nadarajan, R. A., Botnet, H., Using, D., & Learning, A. (2017). HTTP Botnet Detection Using Adaptive Learning Rate Multilayer FeedForward Neural Network To cite this version : HAL Id : hal-01534315 HTTP Botnet Detection using Adaptive Learning Rate Multilayer Feed-forward Neural Network.

[27] Wu, C. H. (2009). Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. Expert Systems with Applications, 36(3 PART 1), 4321–4330. https://doi.org/10.1016/j.eswa.2008.03.002.

[28] Aarthi, J. Design Of Advadvanced Encryption Standard (AES) Based Rijindael Algorithm.