ISP
Innovative Science Publishers

ICSJ
Innovative Computer Science Journal

The efficacy of Deep Learning and Artificial Intelligence framework in enhancing Cybersecurity, Challenges and Future Prospects

Iqra Naseer
IT Cyber Security Manager at Tera Systems Inc. Doha, Qatar

Abstract

This paper stresses the need of recognizing network threats and intrusion detection systems in the ever-changing cybersecurity environment. The paper discusses how increased data transfer rates affect Intrusion Detection Systems (IDS) and how deep learning is vital to cybersecurity. The paper categorizes cyberattacks by their goals and techniques, emphasizing the need for modern defenses. This paper examines the intricate relationships between machine learning, deep learning, and artificial intelligence, describing their roles and strengths and drawbacks. The research shows that machine learning and deep learning can analyze vast datasets, find complicated patterns, and work in real time, making them crucial to cyber risk mitigation. AI technology like ChatGPT may be used in cybersecurity. Exploring cybersecurity challenges, developments, and trends, highlighting the need for modern technologies and the ever-changing cyber threat scenario. As they integrate with new technologies, machine learning and deep learning will improve cybersecurity threat detection and digital identity protection.

Keywords: Cyber-Security, Cyber-Threat, Artificial Intelligence, Deep Learning, Machine learning

Introduction

The increasing integration of the Internet into everyday life is revolutionizing the methods by which individuals engage in studying and working. Nevertheless, it also exposes us to more substantial security vulnerabilities. The prompt highlights the need of promptly addressing and resolving a wide range of network risks, particularly ones that have not been previously seen. (Aftergood, 2017). A network security system encompasses both a network security system and a computer security system as integral components. Numerous components are included inside each of these systems,

including firewalls, antivirus software, and intrusion detection systems (IDS). Intrusion Detection Systems (IDSs) play a crucial role in identifying, evaluating, and acknowledging unauthorized activity inside a system, including actions such as utilization, replication, modification, and eradication (Milenkoski et al., 2015).

Numerous malevolent individuals attempt to undermine login credentials or engage in host data attacks. In recent years, Loukas et al. (2017) have documented several instances of both proofs of concept and occurrences of real-world assaults. Over the years, cyber security analysts Toch et al. (2018) and professionals have developed and established several cyber defence systems to protect organizations' resources from harmful attackers. According to Loukas et al. (2017), these systems are designed to mitigate various cyber security risks, such as viruses, Trojans, worms, and botnets.

Many malicious persons deliberately try to weaken login credentials or carry out host data assaults. Loukas et al. (2017) have recorded many cases of both proofs of concept and real-world attacks in recent years. Over the course of time, scholars and experts in the field of cyber security have devised and implemented several cyber defense systems with the aim of safeguarding an organization's assets from malicious actors (Toch et al., 2018). Loukas et al. (2017) assert that the purpose of these systems is to address and minimize a range of cyber security threats, including viruses, Trojans, worms, and botnets.

Current systems that rely on Intrusion Detection Systems (IDS) use dynamic methods to identify and eliminate vulnerabilities in computer systems, hence initiating appropriate actions for security management. The effectiveness of any assurance instrument relies on its ability to do calculations with high precision and accuracy, enabling efficient processing of the data collected from various sources. In the absence of these capabilities, Intrusion Detection Systems (IDSs) are unable to perform their monitoring and analysis tasks in a continuous manner, hence posing challenges in promptly detecting possible cyber attacks at their onset. This problem arises due to the manner in which current systems exhibit increasingly elevated transmission rates. In a rather rare occurrence, the data transfer rates have increased from 100 Mbps a few years ago to the current data rate of 10CGbps in wired systems. The large amounts of data flowing through systems render IDSs inadequate for the compilation and analysis of each individual system component. Deep Packet Inspection (DPI) tools, such as those developed by Koscher et al. (2010), may effectively operate on wired networks with a maximum bandwidth of 1 Gaps. However, they start to reject packets at a higher speed of 1.5 Gbps due to increased overhead. Checkoway etal., (2011) In their ongoing study, Ward et al. (2013) conducted focused investigations to establish a precise link between performance and the use of Snort and machine learning techniques. They evaluated the effectiveness of these Intrusion Detection Systems (IDS) in handling network traffic at a maximum speed of 10 Gbps. The results of these experiments indicate that the use of

Snort leads to a decrease in regular bundles by 9.5% in 4 Gbps systems, whilst the decrease in normal parcels increases to 20% in 10 Gbps systems. Nevertheless, due to the increase in transfer speed, IDS-based systems that use deep analysis techniques were obliged to progress towards more effective detection methods. McGraw et al. (2013) transitioned from the examination of unprocessed network packets to the analysis of traffic network flows using innovative artificial intelligence techniques.

Smart cyber security laws and systems use deep learning from ANNs. AI can increase cyber risk analytics and organizational resilience, but it has drawbacks. Ensembles and hybrid approaches using deep learning techniques like generative adversarial networks, auto-encoders, multilayer perceptions, convolutional neural networks, recurrent neural networks, long short-term memory, self-organizing maps, and deep belief networks can address cyber security issues. To maximize input-to-output conversion, backpropagation optimizes network weights. Training optimization uses Adaptive Moment Estimation, SGD, and L-BFGS. Neural networks can solve cybersecurity problems. We employ MLP networks to improve IoT systems, assess botnet traffic, construct IDS models, and investigate malware and security issues.MLP hyper-parameters such hidden layers, neurons, and iterations must be carefully adjusted to scale. Xin et al. (2018) say addressing complicated security models is computationally demanding.

Categorization of Cyberattacks

The primary factor in categorizing an assault is the objective of the attack. This phenomenon is often associated with the manner in which an adversary generates revenue from the assault, such as via the acquisition of information and its subsequent sale to advertising or criminal entities (Lala & Panda, 2001). In general, the objectives of the assault may be classified into one of the below groups.

The act of illicitly acquiring information, including data stored on a device, media files, and user credentials, is often executed via the use of spyware software. The act of monitoring users' sensitive data, such as their movements, activities, or health-related information, is often accomplished via the use of mobile malware. The act of seizing control of a system is accomplished by Trojans, botnets, and rootkits, as described by Cristall et al. (2016).

The assault vector adds another level to attack recognition. It is the vulnerability an adversary uses to gain unauthorised access to a network or computer system and perform damaging actions. Attack vectors exist at hardware, network, and application levels. Deep learning technologies are vital to cyber security research, especially intrusion detection. Deep learning is often used to investigate malware and identify unforeseen threats.

Machine Learning and Deep Learning in combating growing cyber threats

The relationship between AI, deep learning (DL), and machine learning (ML) is fraught with mystery. A relatively new academic discipline, artificial intelligence (AI) seeks to model, enhance, and extend human intelligence via the study and development of concepts, approaches, techniques, and applications. In 2017, research was carried out by Smith and Eckroth. A subfield of computer science, artificial intelligence seeks to understand what it means to be intelligent and to create new types of intelligent machines that can mimic human intellect. Robotics, computer vision, expert systems, and natural language processing are all subfields that make up the larger area of research. When it comes to thinking and awareness, AI can mimic human cognitive processes. Though it lacks human intelligence, AI has the potential to outsmart humans in terms of its capacity to mimic human thought processes.

Machine learning (ML) is a subfield of artificial intelligence (AI) that exhibits a tight association with computational statistics, a domain that likewise centers on the utilization of computers for prediction purposes. The discipline is closely associated with mathematical optimizations, since it encompasses many methodologies, theories, and application fields. Machine Learning (ML) is often confused with data mining, as noted by Ashritha and Padmashree (2020). It should be mentioned that the second area, which is often called unsupervised learning, mainly focuses on exploratory data analysis. In addition to acquiring information and constructing basic behavioural patterns for various entities, machine learning may also function autonomously, which can be used to detect major anomalies (Jordan & Mitchell, 2015). When asked to define machine learning, its creator Arthur Samuel said it was a "area of research that enables computers to acquire knowledge without the need for explicit programming." The two mainstays of machine learning (ML)—classification and regression—are dependent on features learned from training data and so already present. In the field of machine learning, DL is still in its early stages. Motivating this effort is the recent breakthrough in neural networks, which can learn analytical tasks by mimicking the way the human brain works. In doing so, it mimics the way the human brain processes and makes sense of a wide variety of data types, including pictures, sounds, and texts (LeCun, Bengio, & Hinton, 2015). Salakhutdinov and Hinton (2009) introduced the notion of deep learning (DL). They developed deep belief networks (DBN) that use an unsupervised greedy layer-by-layer training method. This technique offers a promising solution for handling the optimization issue of deep structures. The following section presents the suggested deep structure of a multi-layer automated encoder. Furthermore, LeCun et al. (1998) introduced the convolutional neural network, which is recognized as the pioneering

multilayer structure learning method. This approach leverages a spatial connection to effectively decrease the parameter count and enhance the training efficiency.

Deep learning (DL) is a machine learning technique that relies on the analysis and interpretation of data. A visual representation, such as an image, may be represented using several methods, such a vector that represents the intensity value of each pixel, or more conceptually as a sequence of edges, an area of a certain form, or similar representations. Accurate representations facilitate the acquisition of new abilities via particular instances. Deep learning strategies include both supervised and unsupervised learning approaches, similar to the techniques used in machine learning. Various learning frameworks provide distinct learning models that exhibit noteworthy variations. According to Deng and Yu (2014), the use of hierarchical feature extraction methods and unsupervised or semi-supervised feature learning in deep learning enables the effective substitution of manual features. The distinctions between ML and DL include the following aspects:

- **Interdependencies among data**. The main difference between deep learning and regular machine learning is how they handle increasing data volumes. Since deep learning algorithms need a large amount of data to get a complete comprehension of the data, their performance degrades when data volumes are constrained. On the other hand, research has shown that standard machine-learning algorithms perform better when they adhere to specified rules. (LeCun, Bengio, & Hinton, 2015).
- **Hardware requirements**. The deep learning method necessitates a sequence of matrix operations. The GPU is mostly used for the effective optimisation of matrix computations. Hence, the GPU is the essential hardware required for the effective functioning of the DL. According to Coelho et al. (2017), deep learning (DL) heavily depends on high-performance computers equipped with GPUs, in contrast to typical machine-learning techniques.
- **Processing of features**. Feature processing is the process of improving the efficiency of learning algorithms by extracting useful patterns from large datasets by integrating domain knowledge into feature extractors. A high level of specialised knowledge is required for the tedious process of feature processing. A data type representation of an application's qualities is often required in machine learning after they have been manually determined by an expert. Features include things like pixel values, shapes, textures, locations, and orientations. The accuracy of the retrieved attributes is crucial to the performance of most machine learning algorithms. When compared to traditional machine learning methods, deep learning's (DL) method of directly extracting high-level features from data stands out (Deng & Yu, 2014). Consequently, DL reduces the need to generate a feature extract for each task.
- **Method for addressing problems**. When using conventional machine-learning algorithms for problem-solving purposes, it is customary for traditional machine

learning to decompose the issue into several sub-problems and then address each sub-problem, finally yielding the ultimate outcome. On the other hand, deep learning promotes the practice of solving problems directly from start to finish.

- **Duration of execution**. Deep learning algorithms include many parameters, making training time-consuming. More time is spent on training. ResNet, the most powerful deep learning algorithm, trains in two weeks, whereas machine learning takes seconds to hours. Unfortunately, the exam is the opposite length. Deep learning algorithms run quickly during testing.

  Unlike other machine learning methods, the test length increases proportionately with data amount. Due to their short testing periods, many machine learning algorithms do not meet this claim. Comparing machine learning (ML) with deep learning (DL) requires interpretability. Deep learning may recognise handwritten numerals as well as humans. However, deep learning systems do not explain their results (Goetz et al., 2015). The mathematical activation of a deep neural network node is evident. What is the best way to represent neurons and how do their layers work together? Thus, explaining how the result was obtained is difficult. However, the machine-learning system provides clear and detailed rules for its decisions, making it easy to explain the result.

Deep Learning and AI in Cybersecurity, detection and prevention and challenges

Machine learning (ML) is a subset of AI that creates algorithms and statistical models to evaluate and predict data. In cybersecurity, machine learning algorithms train on massive datasets to find patterns and anomalies that may suggest vulnerabilities. ML is used in intrusion detection, malware detection, network traffic analysis, and fraud detection in cybersecurity. Machine learning algorithms can detect and mitigate threats faster than rule-based systems using real-time data analysis. Machine learning in cybersecurity has several benefits.

- Machine learning algorithms have the capacity to analyse large amounts of data and detect complex patterns that may be difficult for human analysts to see. According to Yavanoglu and Aydos (2017), possessing this capability may result in an increased degree of accuracy when detecting possible hazards and a decrease in the frequency of erroneous identifications.
- According to Sarker (2021), machine learning algorithms has the capability to analyse data in real-time, hence facilitating expedited identification and reaction to possible dangers.
- Machine learning algorithms streamline several laborious activities related to threat identification and response, enabling human analysts to concentrate on more intricate duties (Xin etal.,2018).

- ML algorithms provide the capability to effectively handle substantial volumes of data, making them very suitable for cybersecurity operations of significant scale (Thomas, Vijayaraghavan, & Emmanuel, 2020).

Cybersecurity Solutions using AI

AI systems like ChatGPT (Chat Generative Pre-Trained Transformer), Google Bard, and Microsoft Bing use various learning strategies to understand and produce text-based responses that resemble human language (Chowdhury et al., 2023). Chatbots and other discussional AI applications use several technologies. This technology is employed in content creation, language interpretation, personal assistants, education, finance and banking, and electronic commerce (Kalla & Smith, 2023). In cyber security, it can recognise and predict complex cyberattacks. NLP models like ChatGPT can be applied in numerous cybersecurity areas. Increase security measures, improve operations, and help cybersecurity professionals are their main goals. Threat analysis, attack detection, access control management, phishing detection, security Chatbots, SIEM, and threat simulation are the challenges mentioned above. ChatGPT has pros and cons like any other technology.

Gundu (2023) proposed a theoretical framework to improve ChatGPT-based information security. The study promoted safe conduct using TPB and Persuasion Theory. Customised interventions including education, training, gamification, security recommendations, reminders, and subtle cues accomplished this. In this situation, ChatGPT provided tailored and engaging instruction on the most effective information security methods. It also offered important warnings and helped perform security evaluations. Gamification was utilised to increase information security knowledge retention and engagement. Furthermore, the use of nudges and reminders effectively facilitated the maintenance of secure behaviours over an extended period.

The potential for malicious exploitation of AI technologies like ChatGPT has been emphasised by Chowdhury et al. (2013). According to the findings of their research, it is posited that ChatGPT has the potential to be used for the generation of detrimental information, hence posing a possible threat to the three essential components of the CIA trinity, namely secrecy, integrity, and availability. The research revealed that the replies generated by ChatGPT sometimes included sensitive information, trade secrets, and copyrighted items, therefore contravening rules of secrecy. Furthermore, the replies provided by the system were not consistently precise, so violating the concept of integrity. Moreover, it is possible to bypass the security measures of ChatGPT in order to generate malevolent code, hence enabling less proficient bad actors or the creation of several hostile attack entities. Once these malicious programmes and materials are developed, there exists a potential for their utilisation on diverse assets in subsequent instances. The possible ramifications of implementing such code application may lead to

catastrophic events, such as the denial of services, hence presenting a substantial risk to the concept of availability in the future.

Renaud et al. (2023) believe that ChatGPT has the potential to be used in the orchestration of intricate assaults. For example, an assailant may use ChatGPT to construct extensively customised spear-phishing communications by using the marketing resources of your organisation. These types of communications have the potential to effectively mislead those who have had comprehensive training in email security awareness due to their lack of resemblance to the conventional suspicious messages they have been taught to recognise. In a different scenario, a bot utilising artificial intelligence had a phone chat with an accounts payable worker, imitating the boss's voice with remarkable accuracy. One possible use of this tactic is to fool or sway those who are unaware of the gravity of the situation. On top of that, cybercriminals can employ AI to successfully customise and contaminate data inside a system, resulting in the creation of a lucrative stock portfolio that can be liquidated prior to the detection of their deceitful activities. These examples exhibit a wide range of variations and may further evolve in complexity if new dangers arise in distinct and more concerning categories as a result of developments in underlying technology. The research undertaken by Al-Hawawreh et al. (2023) examined the ramifications of the ChatGPT model in the field of cybersecurity. Using a case study, they highlighted ChatGPT's impressive practical applications in cybersecurity and showed how it might be used to launch False Data Injection attacks against critical infrastructure like industrial control systems. On the other hand, the authors emphasised the potential of this tool in aiding security analysts in the examination, development, and implementation of security measures aimed at mitigating cyber threats. Moreover, the research investigated the obstacles and potential opportunities linked to ChatGPT within the realm of cybersecurity.

Concerns about privacy, transparency, the dissemination of misleading information, and trust are among the cybersecurity issues linked to this tool's architecture, which researchers must address alongside the tool's ability to create damaging content. Some people are worried about OpenAI's lack of openness in its privacy policy, which just lists the data collected from users and doesn't explain how the company plans to utilise or store that data. Moreover, the policy fails to provide explicit details on the sharing of this data with other entities, hence requiring additional scrutiny and comprehensive examination. Artificial intelligence (AI) solutions, such as ChatGPT, has the capacity to successfully tackle cybersecurity concerns. The use of these tools may facilitate the identification of cyber risks like as phishing attacks, intrusions, malware occurrences, and the execution of vulnerability assessments. Additionally, they can contribute to the provision of staff training. However, there is a potential drawback where these technologies might be used for nefarious intentions, hence increasing cyber vulnerabilities. Within this particular environment, it is possible to modify ChatGPT in a

manner that poses a danger to the confidentiality, integrity, and availability of data. Additionally, it has the capability to write malevolent code, execute advanced cyberattacks, and pose risks to privacy and the dissemination of misleading information. It is essential to acknowledge that while ChatGPT has potential as a helpful instrument in the realm of cybersecurity, its utilisation should be complementary to other security technologies and human experience. It is essential for security professionals to exercise prudence when sharing sensitive information with AI models, while also ensuring that the models are adequately protected and trained for the particular use case. The development of AI tools like ChatGPT is now at its nascent stage, presenting opportunities for enhanced efficacy in addressing cyber security issues.

Challenges, Future Prospects and Emerging Trends

The efficiency and feasibility of present detection systems are being diminished due to the ongoing evolution of cyberattacks. In order to effectively safeguard the digital realm against emerging intelligent assaults, it is imperative to adopt a novel paradigm that diverges from the current ones. Statistical analysis, probability, data mining, ML, DL, and RL are some of the well-established procedures that may be supplemented with AI in this context. Data analysis, interpretation, and trend discovery are the core functions of statistics. The possibility of an event occurring may be measured by its probability. The goal of data mining is to find and isolate unique patterns in massive data sets. Computers can now learn new things with little to no human intervention thanks to machine learning. Data mining, probability-based solutions, and statistics have all had a long history of use in cybersecurity. Reinforcement learning (RL), machine learning (ML), and deep learning (DL) have recently become quite popular in cybersecurity. Improving current attack detection systems by adding new features is possible with the use of techniques drawn from data mining, machine learning, deep learning, and reinforcement learning. Further, these advanced technologies enhance the effectiveness of detecting systems in countering contemporary cyber threats. Probabilistic modelling, decision trees, dimensionality reduction algorithms, boosting-bagging algorithms, regression analysis, and distance-based learning are just a few of the many machine learning techniques used in cybersecurity. In order to identify and prevent data breaches, potential dangers, and vulnerabilities in communication networks and computer systems, machine learning approaches are vital (Aslan et al., 2023).

Fewer human interventions are necessary because to the rapid analysis and adaptation of data by these technologies. Furthermore, machine learning methods greatly enhance network traffic and attack detection accuracy by using heuristic methodologies. As a branch of machine learning, deep learning finds applications in supervised, semi-supervised, and unsupervised learning tasks. More hidden layers are one way in which DL enhances artificial neural networks (ANNs). An input layer, an output layer, and several hidden layers make it up. The field of cybersecurity has made use of many deep

learning models recently. Due to its example-based learning process, DL algorithms need little to no domain expert knowledge. Among the many cybersecurity categories that we identified as having potential for use of deep learning methods were spam and DDoS detection, phishing, anomaly and intrusion detection, and malware and intrusion categorization. Deep learning methods often improve performance while reducing feature space when used to the problem of cyberattack detection. It could be vulnerable to zero-day attacks and evasion, but [4]. Also, deep learning's learning period is long and resource expensive, thus adding hidden layers won't help performance outside of that phase. Despite the many advantages that ML and DL bring to the table when it comes to cyber-attack detection, there are still situations in which it struggles to distinguish attacks from normal network traffic. The issues identified in the study conducted by Ozkan-Ozay et al. (2024) are as follows.

- The detection and prevention of unknown assaults are becoming more difficult.
- The complexity of attacks is increasing.
- Threats are becoming more automated, assuming the form of cyber-attacks-as-a-service.
- Intelligent assaults have the ability to bypass detection systems.
- Machine learning algorithms often make incorrect assumptions about data.
- The categorisation of a vast number of network connections is a significant challenge.
- Managing data with a large number of dimensions may be burdensome.
- Data preparation is complex because of the various formats of the data.
- Developing contextual features poses challenges.
- Applying domain knowledge for automated analysis poses difficulties.
- Testing proposed cybersecurity methods lacks consistent and current datasets.
- Safeguarding multiple components is a complex undertaking.
- Many different paths constitute the assault vector.
- Ransomware assaults are becoming more advanced.
- Methods used in social engineering are dynamic and ever-changing.

The area of cybersecurity is increasingly incorporating emerging technologies such as blockchain, virtualization, cloud computing, and big data. Blockchain technology facilitates the verification of the precision in identifying various intricate threats. Virtualization technology is a method that effectively separates software programmes from their underlying hardware components, therefore improving software flexibility, saving expenses, and mitigating the impact of cyber assaults by minimising downtime. Cloud computing provides proactive measures to mitigate threats, ensures strong availability, allows for scalability, facilitates efficient data recovery, and offers better data security. The use of big data may facilitate the analysis of vast datasets to reveal previously unidentified trends in characteristics that are suggestive of malicious

activities. A safety-critical detection system is anticipated to perform better with the use of AI methods like ML and DL, as well as new technologies such as virtualization, which is blockchain technology, big data, and cloud computing.

Conclusion

The methodologies of Machine Learning and Deep Learning are influenced by the impressive ability of the human brain to efficiently learn information from previous experiences. These approaches have been widely adopted by other fields of study to address their own problems. The increasing popularity of internet use and the wide array of network applications have led to a heightened awareness in the subject of cyber security. This study provides a comprehensive review of the literature on various deep learning and machine learning approaches used in cyber security assaults. ChatGPT and other AI, ML, DL, and RL technologies are great at reducing attacks. People, businesses, and other entities may strengthen their data security in the face of a constantly changing threat landscape by using these technologies. Given the persistent focus on cybersecurity, it is anticipated that machine learning technologies will assume an increasingly prominent role in protecting digital identities. The integration of other technologies, including as blockchain, virtualization, cloud computing, and big data, with machine learning methodologies, is likely to result in improved performance of the detection system.

References

Aftergood, S. (2017). Cybersecurity: The cold war online.

Al-Hawawreh, M., Aljuhani, A., & Jararweh, Y. (2023). Chatgpt for cybersecurity: practical applications, challenges, and future directions. *Cluster Computing*, *26*(6), 3421-3436.

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th international conference on cyber Conflict (CyCon)* (pp. 371-390). IEEE.

Ashritha, S., & Padmashree, T. (2020). Machine learning for automation software testing challenges, use cases advantages & disadvantages. *International Journal of Innovative Science and Research Technology*, *5*(9).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX security symposium (USENIX Security 11)*.

Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., & Rahman, M. S. (2023, May). ChatGPT: A threat against the CIA triad of cyber security. In *2023 IEEE International Conference on Electro Information Technology (eIT)* (pp. 1-6). IEEE.

Coelho, I. M., Coelho, V. N., Luz, E. J. D. S., Ochi, L. S., Guimaraes, F. G., & Rios, E. (2017). A GPU deep learning metaheuristic based model for time series forecasting. *Applied Energy*, *201*, 412-418.

Cristalli, S., Pagnozzi, M., Graziano, M., Lanzi, A., & Balzarotti, D. (2016). Micro-virtualization memory tracing to detect and prevent spraying attacks. In *25th {USENIX} Security Symposium ({USENIX} Security 16)* (pp. 431-446).

Deng, L., & Yu, D. (2014). Deep learning: methods and applications. *Foundations and trends® in signal processing*, *7*(3–4), 197-387.

Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, *28*, 2861-2879.

Goetz, J. N., Brenning, A., Petschko, H., & Leopold, P. (2015). Evaluating machine learning and statistical prediction techniques for landslide susceptibility modeling. *Computers & geosciences*, *81*, 1-11.

Gundu, T. (2023, July). Chatbots: A framework for improving information security behaviours using ChatGPT. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 418-431). Cham: Springer Nature Switzerland.

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255-260.

Kalla, D., & Smith, N. (2023). Study and Analysis of Chat GPT and its Impact on Different Fields of Study. *International Journal of Innovative Science and Research Technology*, *8*(3).

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010, May). Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy* (pp. 447-462). IEEE.

Lala, C., & Panda, B. (2001). Evaluating damage from cyber attacks: a model and analysis. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *31*(4), 300-310.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *nature*, *521*(7553), 436-444.

LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, *86*(11), 2278-2324.

Li, C., & Qiu, M. (2019). *Reinforcement learning for cyber-physical systems: with cybersecurity case studies*. CRC Press.

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, *6*, 3491-3508. https://doi.org/10.1109/ACCESS.2017.2782159

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, *6*, 3491-3508.

McGraw, G. (2013). Cyber war is inevitable (unless we build security in). *Journal of Strategic Studies*, *36*(1), 109-119.

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., & Payne, B. D. (2015). Evaluating computer intrusion detection systems: A survey of common practices. *ACM Computing Surveys (CSUR)*, *48*(1), 1-41.

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*.

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*.

Renaud, K., Warkentin, M., & Westerman, G. (2023). *From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI*. MIT Sloan Management Review.

Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, *2*(3), 154.

Smith, R. G., & Eckroth, J. (2017). Building AI applications: Yesterday, today, and tomorrow. *Ai Magazine*, *38*(1), 6-22.

Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. (2020). *Machine learning approaches in cyber security analytics* (pp. 37-200). Singapore: Springer.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR)*, *51*(2), 1-27.

Ward, D., Ibarra, I., & Ruddle, A. (2013). Threat analysis and risk assessment in automotive cyber security. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems*, *6*(2013-01-1415), 507-513.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381.

Yavanoglu, O., & Aydos, M. (2017, December). A review on cyber security datasets for machine learning algorithms. In *2017 IEEE international conference on big data (big data)* (pp. 2186-2193). IEEE.