International Journal of communication and computer Technologies, Vol. 12, No. 1 , 2024 (pp. 38-44) IJCCTS
RESEARCH ARTICLE WWW.IJCCTS.ORG

Use of machine learning for the detection, identification, and mitigation of cyber-attacks

Dr. **Waleed S. Alnumay**

Computer Science Department, Riyadh Community College, King Saud University, Riyadh, Saudi Arabia
Email: wnumay@ksu.edu.sa

Keywords:
Machine learning,
detection,
identification,
mitigation,
cyber-attacks

DOI: 10.31838/IJCCTS.12.01.05

Received: 13.01.2024

Accepted: 11.02.2024

Publication: 04.03.2024

Abstract

With the increased use of internet services for various public and private purposes, the threat of cyber-attacks is also increasing. Machine learning methods are effective against these threats. This paper aims to review these methods in terms of their utility for the detection, identification, and mitigation of cyber-attacks now and in the future.

Many reviews described and discussed various machine learning methods and how each method can be used against specific types of cyber threats. However, empirical evidence did not show any clear superiority of one method over the others. The differences in research contexts and methodologies could have contributed to this uncertainty. However, deep learning methods might have an edge over shallow learning methods.

Emerging new trends of cyber-attacks demand renewed research on the problem. The invention of an entirely new concept to deal with various cybersecurity issues cannot be ruled out.

How to cite this article: Alnumay WS (2024). Use of machine learning for the detection, identification, and mitigation of cyber-attacks. International Journal of communication and computer Technologies, Vol. 12, No. 1, 2024, 38-44

Introduction

Till about the 1970s, cyber security was limited to academia. However, with the advent of the internet, cyber threats began to happen due to a large number of public and private organisations, and the public increasingly uses it for various types of communications. Such increased connectivity led to attacks involving computer viruses and network intrusions. Thus, the age of cyber threats and security started. The average global cost of a data breach in 2020 was 3.86 million USD. These costs included the expenses incurred in discovering and responding to the breach, the downtime losses, the lost revenue, and the long-term damage to the business and brand reputation.(IBM, 2023).

Some instances of cyber attacks

In one of the earliest attempts to collate the efforts on cyber security issues, in 1967, a session organised by Willis Ware at the Spring Joint Computer Conference, and the later publication of the Ware Report in 1970 stressed the intersection of material, cultural, political, and social concerns on this issue (Misa, 2016). A NIST publication of 1977 (Ruthberg & McKenzie, 1977) introduced the CIA triad of confidentiality, integrity, and availability as a clear and simple way to describe key security goals. This framework was enlarged by many in later years.

One of the earliest attacks on a computer network was the computer worm Creeper written by Bob Thomas at BBN. This was propagated through the ARPANET in 1971. The program was only experimental without any malicious payload. Later, a programme, Reaper, was created by Ray Tomlinson in 1972 to destroy Creeper.

A group of German hackers led by Markus Hess attempted the first recorded cyber espionage from September 1986 to June 1987. The group hacked into American defence contractors, universities, and military base networks and sold the information so gathered to the Soviet KGB. The group was arrested on 29 June 1987 and convicted of espionage on 15 February 1990.

The Morris worm, one of the computer worms, received significant media attention in 1988 as it

spread through the internet. In 1993, Netscape began developing the SSL protocolshortly after the National Centre for Supercomputing Applications (NCSA) introduced the first web browser, Mosaic 1.0. However, Netscape withheld its version 1.0 release from the public due to numerous critical security flaws, such as replay attacks and the potential for hackers to modify unencrypted communications from users. It wasn't until February 1995 that Netscape finally released Version 2.0.

Many times offensive strategies of cyberattacks against adversaries fail when the adversary also develops such capabilities. Such failure of strategies happened in the case of the National Security Agency of the USA against its adversaries like Russia, Iran and North Korea(Perlroth, 2021). The author uses many examples of US intelligence failures to prove this point.

Definition of cyber security

Cyber security involves utilising technologies, procedures, and measures to safeguard systems, networks, software, devices, and information from malicious cyber threats. Its goal is to mitigate the chance of cyber-attacks and safeguard against unauthorised intrusion into systems, networks, and technologies.

(ITGovernanceLtd, 2023).

Cybersecurity is the act of safeguarding systems, networks, and software from online assaults. These digital assaults typically target sensitive data, seek monetary gain from users, or disrupt regular business operations. Keeping networks secure is especially difficult in today's world, where there are more devices than people, and attackers are constantly developing new methods. (Cisco, 2023).

Cybersecurity is the act of safeguarding vital systems and confidential data from online assaults. It is also referred to as IT security, and it involves implementing measures to defend against potential dangers to networked systems and programs, regardless of whether they stem from within or outside an institution. (IBM, 2023).

An examination of the above definitions shows that all of them have similar meanings. Any of these definitions can be used when considering machine learning methods for cybersecurity.

This paper aims to provide a qualitative review of the current status of the use of machine learning methods in cybersecurity.

Method and Results

Method

A comprehensive literature search was conducted on Google Scholar to identify relevant studies related to the use of machine learning for the detection, identification, and mitigation of cyber-attacks from 2014 to 2023. Keywords used for the search included "machine learning", "cyber-attacks", "cybersecurity", "intrusion detection", "anomaly detection", and "cyber threat intelligence". The search was limited to articles published between 2014 and 2023 to provide an updated review of the current state of research in this field.

The following inclusion criteria were applied to select relevant studies for the review: 1) studies that used machine learning techniques for detecting, identifying, or mitigating cyber-attacks; 2) articles written in English; and 3) studies published between 2014 and 2023. Studies were excluded if they did not meet the inclusion criteria or if they were not available in full text. Studies that focused on other areas of cybersecurity, such as encryption or network security, were also excluded.

The results obtained are discussed below.

Results

Use of machine learning for cybersecurity

Machine learning is a category within the broader field of artificial intelligence (AI). AI is the ability of a machine to simulate intelligent behaviour like that of a human. AI technology is utilised to accomplish complicated tasks in a manner similar to how humans tackle problems.The four basic machine learning methods are supervised learning, unsupervised learning, semi-supervised learning, and reinforced learning.

Soni and Bhushan (2019)noted that cyber security can adopt machine learning to cross the limitations of the traditional rule-based algorithms for greater efficiencythrough their integration with AI. Although complete automation of analysis and detection may be a distant goal, significant parts of cyber security can be improved using machine learning methods.The usefulness of AI for cyber security was highlighted by Prasad and Rohokale (2020). Amit, et al. (2018)observed that to solve cybersecurity problems, certain machine learning challenges need to be addressed. The first challenge is malware

detection and classification. Many threat intelligence repositories are based on signatures of the malware. So, it is possible to use a slight modification to detect signature-based detection. The most commonly used algorithms for this purpose are Naive Bayes Classifier, Support Vector Machine(SVM), Random Forest (Hu & Tan, 2017b),DotNetNuke(DNN), Convolutional Neural Network(CNN) andLong Short Term Memory(LSTM).

Different machine learning methods

Different machine learning methods used for cyber security were discussed by Apruzzese, Colajanni, Ferretti, Guido, and Marchetti (2018). The authors classified machine learning methods into shallow and deep learning, and each of them was further divided into supervised and unsupervised learning. Under supervised slow learning (SL) algorithms, Naïve Bayes (NB), Logistic Regression (LR), Support Vector Machines (SVM), Random Forest (RF), Hidden Markov Models (HMM), K-Nearest Neighbours (KNN), and Shallow Neural Network (SNN) were included. Under unsupervised SL algorithms, clustering and association were included. Under supervised deep learning (DL) algorithms, Fully connected Feedforward Deep Neural Networks (FNN), Convolutional Feedforward Deep Neural Networks (CNN), and Recurrent Deep Neural Networks (RNN) were included. Under unsupervised DL algorithms, Deep Belief Networks (DBN) and Stacked Autoencoders (SAE) were included. Each of these has been described briefly. Applications of these ML algorithms for intrusion detection, malware analysis, and spam detection have been tabulated. Some issues related to these applications have also been highlighted.

In a review, Berman, Buczak, Chavis, and Corbett (2019) discussed various machine learning methods used for various cybersecurity issues with the help of diagrams. These included the comparison of shallow (ANN) and deep learning, and deep learning methods like deep belief networks, deep autoencoders, restricted Boltzmann machines, recurrent neural networks, convolutional neural networks, generative adversarial networks and recursive neural networks. Deep learning methods are useful for the detection and classification of malware, domain generation algorithms and botnet detection, drive-by-download attacks, network intrusion detection, file type identification, network traffic identification, spam identification, insider threat identification, border gateway protocol anomaly detection, verification if keystrokes were typed by human, user authentication and false data injection attack detection. Due to the differences in methods and contexts, comparisons to arrive at the most suitable method for any type of cyber threat are difficult. In future research, there is a need to consider the cascading connection of malicious activities throughout an attack lifecycle, rather than each in isolation.

Through a literature survey, Das and Morris (2017) discussed some machine learning applications (Bayesian Networks, Decision Trees, Clustering, Artificial Neural Networks, Genetic algorithms and genetic programming, Hidden Markov Models, and Inductive Learning) for cyber analytics for intrusion detection, traffic classification and applications like email filtering. ML is used in cyber security in three main ways. Clustering algorithms (Density-based like DBSCAN) and SVM are the best methods for anomaly detection. For misuse detection, the classifiers can generate signatures. The branch features in a decision tree or chromosomes in a genetic algorithm generate signatures that are more suitable for misuse detection. Therefore, algorithms like ANN and SVMs with hidden nodes are not suitable for misuse detection. The authors used MODBUS data to compare Naïve Bayes, Random Forest, One R, and J48. The area under the curve was the highest for J48. However, more tests are required to confirm this.

Different critical aspects related to Deep Reinforced Learning-based security methods for cyber-physical systems, autonomous intrusion detection techniques and multiagent DRL-based game theory simulations for defence strategies against cyber-attacks were discussed by Nguyen and Reddi (2021). The authors also discussed some newly emerging types of attacks on which more research is recommended.

Aspects of cyber security and the use of machine learning methods

Different applications of machine learning techniques in cyber security were discussed by Ford and Siraj (2014). The aspects covered were phishing and fraud, network intrusion, testing securityproperties of protocols, authentication with keystroke dynamics, cryptography, human interaction proofs, spam detection in social networks, smart meter energy consumption profiling, and issues in the security of machine learning techniques. In all these aspects, many researchers have compared different machine learning methods to detect, prevent and correctcyber

security problems. However, machine learning itself may be subject to attacks like causative attacks altering the training process, attacks on integrity and availability, making falsepositives as a breach into a system,exploratory attacksexploiting the existing vulnerabilities, targeted attacksdirected to a certain input, indiscriminate attacks inwhich inputs fail. Defences against a few of these have been developed using different frameworks.

(Yavanoglu & Aydos, 2017)reviewed the datasets used by researchers to develop and test ML methods for cyber security. The data sets included KDD Cup 1999 Dataset (DARPA1998), ECML-PKDD 2007 Dataset, ISOT (Information Security and Object Technology) Dataset, HTTP CSIC 2010 Dataset, CTU-13 (Czech Technical University) Dataset, The ADFA Datasets, andUNSW-NB15 Dataset.

A study conducted by Ferrag et al. (2020) examined intrusion detection systems utilising deep learning strategies andclassified 35 data sets across seven categories, including network traffic, electrical networks, internet traffic, virtual private networks, android apps, IoT traffic, and internet-connected devices.The study also compared seven types of deep learning models using two new real traffic data sets, CSECIC-IDS2018 and Bot-IoT, for both binary and multiclass classification purposes. Their comparative performance in terms of false alarm rate, accuracy, and detection rate varied with the type of data set.

A maximum-minimum normalisation was performed by Kilincer, Ertam, and Sengur (2021) on CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD and CIDDS-001 data sets and their classification was made using SVM, KNN, and DT algorithms. Success rates of99.81%, 99.18% and 99.92% success rates were obtained for the three algorithms, respectively, with the CSE-CIC-IDS 2018 data sets.

Specific research works

In the case of cyber-attacks against a power system, human judgment is difficult. This is due to the overt attempt to disguise the attack and deceive the operators regarding the true state of the system. To enable the human decision-maker, Hink, et al. (2014)evaluated the viability of machine learning to discriminate types of power system disturbances, and focus specifically on detecting cyber-attacks where deception is the core issue. The original benchmarks were put in place to use machine learning methods for identifying power system disturbances within a smart power grid structure. Out of the machine learning algorithms, the use ofthe JRipper+Adaboost method over a three-class (Attack, Natural Disturbance, and No Event) classification scheme enabled reliable classification of power system disturbances with low false positive rates.

Ferrag, Friha, Maglaras, Janicke, and Shu (2021) presented a comprehensive study in which an experimental analysis was done on cyber security in the Internet of Things (IoT) applications, using federated deep learning approaches. RNN, CNN and DNN were compared. Three new real IoT traffic datasets, the Bot-IoT dataset, the MQTTset dataset, and the TON_ IoT dataset, were used. The highest accuracy for the Bot-IoT dataset was obtained using the RNN classifier, which achieved 96.76%, while the lowest accuracy was obtained using the DNN classifier, with 95.76%. In the case of centralised learning models, for the MQTTset dataset, the highest accuracy was obtained using the DNN classifier, which achieved 90.06%, while the lowest accuracy was obtained using the RNN classifier, with 89.29%. The RNN classifier had the greatest precision for the TON_IoT dataset at 99.98%, whereas the CNN classifier had the lowest precision at 98.87%. In the case of federated learning models, the best method was the integration ofblockchain technology with its cyber security in IoT networks. Threat reduction improved and enabled data owners tohave better control over the access to stored and shared data. Federated deep learning approaches (CNN, RNN, and DNN) outperformed the classiccentralised versions of machine learning (non-federated learning) to ensure the privacy of IoT device data and to provide higher accuracy in detecting attacks.

Frameworks and modelsusing machine learning

Conventional methods, like static and binary analysis of malware, are inefficient in addressing the escalation of malware due to the time taken to reverse engineer the binaries to create signatures. A signature for the malware is accessible,though the malware might have caused significant damage to the system.Leveraging the benefits of machine learning algorithms, Vinayakumar, Soman, Poornachandran, and Menon (2019) proposed a method termed Deep-DGA Detect/Deep-URL. In this method, raw domain names/URLs are encoded using character-level embedding, which is a natural language processing method. In experiments, The deep-learning

methods performed well compared to the traditional machine-learning classifiers in all tests. Convolutional neural network-long short-term memory (CNN-LSTM) performed best among all deep learning methods tested. The proposed framework is highly scalable and is named the Deep Cyber Threat Situational Awareness Framework (DCTSAF).This framework can handle two million events per second,analyse large volumes and types of data, and perform almost a real-time analysis to provide early warning about malicious activities.

An intrusion detection model based on machine learning, IntruDTree, was presented bySarker, Abushark, Alsolami, and Khan (2020). The model-first considers the ranking of security features based on their importance and then builds a tree-based generalised intrusion detection model using the selected important features. The model was effective for the prediction accuracy for unseen test cases. It also minimised the computational complexity by reducing the feature dimensions. Experiments comparing with other machine learning models like naive Bayes classifier, logistic regression, support vector machines, and k-nearest neighbour showed IndruDTree to be superior to all of them in terms of precision, recall, Fscore and accuracy.

Roopak, Tian, and Chambers (2019)proposed deep learning models for cyber security in IoT (Internet of Things) networks.The models were evaluated using the latest CICIDS2017 datasets for DDoS attack detection. An accuracy of 97.16% was obtained for the proposed models, which was higher than other machine learning algorithms.

Discussion an Conclusions

In recent years, the emergence and evolution of cyber threats have posed significant challenges to the security of information and communication systems. Traditional methods of protection and detection have become increasingly inadequate in the face of ever-evolving attack strategies. This has led to a growing interest in the use of machine learning techniques as a means to enhance cyber security. Through this paper, we have examined the use of machine learning for the detection, identification, and mitigation of cyber-attacks.

Based on our examination of past articles, it is clear that machine learning techniques have been widely utilised in the field of cyber security. Numerous studies have investigated the effectiveness of various machine learning approaches, including deep learning, support vector machines, and random forests, in tackling a range of cyber threats. These methods have demonstrated success in detecting and preventing attacks, as well as identifying abnormal patterns in network data.

However, there are significant differences in the research contexts and methodologies used in these studies, making it challenging to determine the most effective method for addressing specific aspects of cyber threats. Despite this, our analysis suggests that deep learning methods have shown an edge over shallow learning methods in terms of accuracy and efficiency. This is likely due to deep learning's ability to learn complex patterns from large datasets, making it suitable for identifying and analysing the behaviours of sophisticated cyber-attacks.

Also, with the rapid emergence of new cyber threats, there is a constant need for the development of new and adaptive methods to ensure effective protection. Machine learning techniques have the potential to continuously evolve and adapt to new threats, making them a valuable tool in the fight against cybercrime. Future research efforts should focus on exploring and developing innovative machine learning methods to address emerging cyber threats.

In conclusion, our review has shown the significant progress made in the use of machine learning techniques for cyber security. These methods have proven to be effective in detecting, identifying, and mitigating various forms of cyber-attacks. However, there is still room for improvement, and further research is needed to develop more robust and efficient methods. Additionally, the creative application of machine learning concepts could potentially lead to ground-breaking advancements in cyber security. As such, the use of machine learning in cyber security is a field that continues to hold much promise and potential for future development.

References

1. Amit, I., Matherly, J., Hewlett, W., Xu, Z., Meshi, Y., & Weinberger, Y. (2018). Machine learning in cyber-security-problems, challenges and data sets. *arXiv, 1812*, 07858. doi:10.48550/arXiv.1812.07858
2. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In T. Minárik, R. Jakschis, & L. Lindström (Ed.), *2018 10th internation-*

al conference on cyber Conflict (CyCon), 29 May 2018 - 1 June 2018, Tallinn, Estonia (pp. 371-390). IEEE. doi:10.23919/CYCON.2018.8405026

3. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information, 10*(4), 122. doi:10.3390/info10040122
4. Cisco. (2023). *What Is Cybersecurity?* Retrieved February 1, 2023, from Cisco: https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html#~related-topics
5. Das, R., & Morris, T. H. (2017). Machine learning and cyber security. *International conference on computer, electrical & communication engineering (ICCECE), 22-23 December 2017, Kolkata, India* (pp. 1-7). IEEE. doi:10.1109/ICCECE.2017.8526232
6. Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEE Access, 9*(October), 138509-138542. doi:10.1109/ACCESS.2021.3118642
7. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50* (February), 102419. doi:10.1016/j.jisa.2019.102419
8. Ford, V., & Siraj, A. (2014). Applications of machine learning in cyber security. *Proceedings of the 27th international conference on computer applications in industry and engineering, Kota Kinabalu, Malaysia.118*, pp. 1-6. IEEE Xplore. Retrieved February 1, 2023, from https://vford.me/papers/Ford%20Siraj%20Machine%20Learning%20in%20Cyber%20Security%20final%20manuscript.pdf
9. Hink, R. C., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014). Machine learning for power system disturbance and cyber-attack discrimination. *7th International symposium on resilient control systems (ISRCS), 19-21 August 2014, Denver, CO, USA* (pp. 1-8). IEEE. doi:10.1109/ISRCS.2014.6900095
10. IBM. (2023). *What is cybersecurity?* Retrieved February 1, 2023, from IBM: https://www.ibm.com/in-en/topics/cybersecurity
11. IT Governance Ltd. (2023). *What is Cyber Security? Definition and Best Practices.* Retrieved February 1, 2023, from IT Governance Ltd, UK: https://www.itgovernance.co.uk/what-is-cybersecurity
12. Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks, 188*(April), 107840. doi:10.1016/j.comnet.2021.107840
13. Misa, T. J. (2016). Computer Security Discourse at RAND, SDC, and NSA (1958-1970). *IEEE Annals of the History of Computing, 38*(4), 12 - 25. doi:10.1109/MAHC.2016.48
14. Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*(November), 1-17. doi:10.1109/TNNLS.2021.3121870
15. Perlroth, N. (2021, February 11). *How the United States Lost to Hackers.* Retrieved February 1, 2023, from New York Times: https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html
16. Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. In *Cyber security: the lifeline of information and communication technology* (Vol. Springer Series in Wireless Technology (SSWT), pp. 231-247). Springer, Cham. doi:10.1007/978-3-030-31703-4_16
17. Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. *9th annual computing and communication workshop and conference (CCWC), 7-9 January 2019, Las Vegas, NV, USA* (pp. 452-457). IEEE. doi:10.1109/CCWC.2019.8666588
18. Ruthberg, Z. G., & McKenzie, R. G. (1977). *COMPUTER SCIENCE & TECHNOLOGY: Audit and Evaluation of Computer Security.* Department of Commerce. National Bureau of Standards. Retrieved February 1, 2023, from https://web.archive.org/web/20161010044638/http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf
19. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry, 12*(5), 754. doi:10.3390/sym12050754
20. Soni, S., & Bhushan, B. (2019). Use of Machine Learning algorithms for designing efficient cyber security solutions. *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 5-6 July 2019, Kannur, India.1*, pp. 1496-1501. IEEE. doi:10.1109/ICICICT46008.2019.8993253
21. Vinayakumar, R., Soman, K. P., Poornachandran, P., & Menon, V. K. (2019). A deep-dive on machine learning for cyber security use cases. In *Machine Learning for Computer and Cyber Security* (1st ed., pp. 122-158). CRC Press. Retrieved February 1, 2023, from https://www.taylorfrancis.com/chapters/edit/10.1201/9780429504044-6/deep-dive-machine-learning-cyber-security-use-cases-vinayakumar-soman-prabaharan-poornachandran-vijay-krishna-menon
22. Yavanoglu, O., & Aydos, M. (2017). A review on cyber security datasets for machine learning algorithms. *IEEE international conference on big data (big data), 11-14 December 2017, Boston, MA, USA* (pp. 2186-2193). IEEE. doi:10.1109/BigData.2017.8258167
23. Mukti, Ishrat Zahan, Ebadur Rahman Khan, and Koushik Kumar Biswas. "1.8-V Low Power, High-Resolution, High-Speed Comparator With Low Offset Voltage Implemented in 45nm CMOS Technology." Journal of VLSI circuits and systems 6.1 (2024): 19-24.

24. Khan, Mohammad Nazrul Islam, and Riyaz Ahmad Khan. "Liftings from Lorentzian para-Sasakian manifolds to its tangent bundle." Results in Nonlinear Analysis 6.4 (2023): 74-82.

25. MOHAMMADZADEH, ALI, and BJ ADAMS. "State of art design of novel adder modules for future computing." International Journal of communication and computer Technologies 11.2 (2023): 53-67.