STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Machine Learning for Cybersecurity Issues : A systematic Review

Aseel Alshuaibi, Mohammed Almaayah[2] and Aitizaz Ali[3]

[1] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[2] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*
[3] *Network Security Forensic Group, School of Technology, Asia Pacifc University, Malaysia*

ARTICLE INFO

Article History

Received 23 Jan 2025
Accepted 19 Feb 2025
Published 20 Feb 2025

Academic Editor:

Youakim Badr

Vol.2025, No.1

DOI:

https://doi.org/10.63180/jcsra.thestap.2025.1.4

ABSTRACT

With growing of the usage of the Information technologies and social networks, the identification of different network attacks, especially those not previously discovered, is an important concern that needs to be addressed. This paper is reviewing recent studies on security incidents and related security issues. The aim of the study is to clarify how Machine Learning techniques can influence cybersecurity. Moreover, this study aims to analyze and review previous studies related to machine learning (ML) and how could ML techniques improve the security. In addition, it will discuss and highlight different applications of ML in cybersecurity. As well as understand the use of ML in addressing some of cybersecurity problems. After reviewing previous studies and analyzing the results, the results show that machine learning are positively change the cybersecurity field. By mapping major machine learning algorithms with cyber-attacks and discuss the effectiveness of each algorithm for corresponding attack.

Keywords: Internet of Things (IoT); Cybersecurity; Cyber-attacks; IoT Assets and Threats.

How to cite the article

Alshuaibi, A., Almaayah, M., & Ali, A. (2025). Machine Learning for Cybersecurity Issues : A systematic Review. Journal of Cyber Security and Risk Auditing, 2025(1), 36–46. https://doi.org/10.63180/jcsra.thestap.2025.1.4

1. Introduction

With the growing of deep usage of the Internet, technology and social networks, the way people learn, and work is rapidly changing. Thus, disclose the people to growingly significant security threats [1]. The identification of different network attacks, especially those not previously discovered, is an important concern that needs to be addressed. The objective of the research is to work on cybersecurity data science by discussing recent information on security incidents and related security services. In addition, clarifying how Machine Learning techniques can influence cybersecurity and exploring the security challenges [1] [2].

Cybersecurity is a collection of technologies aimed at preventing cyber attackers and unauthorized entry, modification or disclosure of devices, networks, applications, and information [1]. In the sense of computing, cybersecurity is experiencing major changes in technology and its operations, and data science (DS) is driving the transition where Machine Learning (ML), a key component of "Artificial Intelligence," will take an important role in discovering data insights. Machine learning will positively change the cybersecurity field. These related technologies are rapidly growing recently [2].

Machine Learning (ML) is a subset of artificial intelligence that is closely linked to computational statistics, data mining and analytics, and data science, with an emphasis on teaching machine to learn from data [1][2]. Moreover, Machine

Learning models are made up of a series of laws, processes, or complicated "transfer functions" that can be used to find meaningful data patterns as well as predict actions, and that can be useful in the field of cybersecurity [2].

Data science is changing industries around the world. "Security is all about data", thus, data science is important for the development of intelligent cybersecurity systems. Security data are analyzed in the form of files, logs, network packets, when cyber threats need to be detected. Security experts have commonly not used data science techniques to establish incidences. File hashes, custom-written rules such as signatures, or manually defined heuristics were instead used. In some cases, while these methods have their own benefits, too much manual work is required to deal with the evolving cyber threat environment [2]. Thus, data science will cause a major change in technology and its practices. Machine Learning algorithms and methods can be used to learn or derive information from the training data for their detection and prevention of security incident patterns. For example, it is possible to use these techniques to detect malware or unusual patterns, as well as extraction of policy rules [2].

In recent years, different security attacks such as unauthorized access, malware attack, zero-day attack, security breach, denial of service, social engineering and much more have risen at an increasing rate due to the growing reliance on digital technology and Internet-of-Tings. Cybercrime and attacks can result in serious financial losses and can harm organizations and individuals. In addition to the rapid growth of web and mobile technologies, attack methods are also becoming more advanced and complex in breaching systems and networks. Machine Learning approaches and techniques provide possible solutions that can be used because of their ability to adapt rapidly to new and unfamiliar conditions to overcome such difficult and complex situations [2] [3]. In order to solve wide-ranging computer and information security issues, numerous Machine Learning techniques have been successfully implemented. This paper explores and highlights various applications of Machine Learning in cyber security [3]. The objective of the research is to work on cybersecurity data science by discussing recent information on security incidents and related security services. In addition, clarifying how Machine Learning techniques can influence cybersecurity and exploring the security challenges [2]. Based on the research goal and review of literature, the following research questions are developed to guide the investigation:

Research Question 1: What are the possible Machine Learning techniques that could be used for improving Cybersecurity?
This question will identify the possible ML techniques and methods that can be used to improve and robust the cybersecurity.

Research Question 2: What are the possible cyber-attacks that can be reduced using Machine Learning techniques?
This question will identify the possible cyber-attacks and threats that ML techniques can address to improve the cybersecurity.

Research Question 3: How effective are the various types of Machine Learning techniques in improving the Cybersecurity?
This question will identify how ML techniques improve and robust the cybersecurity. Also, it will discuss and highlight different applications of ML in cybersecurity.

This paper is a review of previous studies to address the cybersecurity issues and the use of Machine Learning techniques to solve them. It consists of three milestones and it will be completed by the end of this semester. It will be implemented in English language. The project will be determined successful if Machine Learning techniques support the development of intelligent cybersecurity systems. The only constraint that might be faced is the limitation of recent research studies relating to this field.

2. Literature Review

The main goal of this section is to present an overview of the literature of machine learning in cybersecurity, which has been done concerning Machine Learning techniques in Cybersecurity, as shown in Table 1. The aim is to find what are the different types of Machine Learning techniques that could be applied to improve ccybersecurity. Several studies and literature reviews exist in the area of Cybersecurity and machine learning, for instance, [1] performed a survey paper on Machine Learning and Deep Learning Methods for Cybersecurity. The core literature surveys on machine learning (ML) and deep learning (DL) methods for network analysis of intrusion detection are described in this survey paper, it includes a brief tutorial summary of each ML/DL processes. The result of the discussion of comparisons among the different approaches reveals that each solution to applying an intrusion detection scheme has its own set of advantages and drawbacks. As a result, deciding which approach to use to enforce an intrusion detection scheme is challenging. [2] Provided a survey paper on Cybersecurity

data science, an overview from machine learning perspective. This survey paper concentrates on and briefly analyze cybersecurity data science, in which data is collected from relevant cybersecurity sources and algorithms are used to supplement the current data-driven trends to have more effective protection solutions. The authors successfully produce a multi-layered machine learning-based architecture for cybersecurity modeling.

[3] Performed a conference paper on applications of Machine Learning in Cybersecurity. This paper examines and outlines various machine learning techniques of cyber security. This research looks at phishing identification, network intrusion detection, checking protocol protection properties, authentication with keystroke mechanics, encryption, human interface proofs, spam detection in social networks, smart meter energy usage profiling, and security problems with machine learning techniques. [4] Published a conference paper on Machine Learning and Cybersecurity. This paper is a review of the literature on machine learning and its implementations in cyber analytics, including intrusion detection, traffic classification, and email filtering. It provided suggestions for when to use a particular algorithm. Moreover, the paper analyzed four machine learning algorithms on MODBUS data gathered from a gas pipeline. ML algorithms were used to classify various attacks, and the performance of each algorithm was then evaluated. The result of this paper shows that the analysis found that the J48 algorithm has the best performance among all algorithms. Also, because of its optimum real-time efficiency, Random forest could be a better choice as a key IDS algorithm. [5] Produced a conference paper on the Effectiveness of Machine and Deep Learning for Cyber Security. An overview and analysis of machine learning approaches used to detect intrusion, ransomware, and spam is provided and addressed to security professionals. The aim is to determine the effectiveness of these technologies and to recognize the major constraints that prevent machine learning cyber detection schemes from being implemented immediately. The paper findings show that current machine learning approaches have several flaws that limit their effectiveness in terms of cyber defense.

[6] Provided a conference paper on Machine Learning for Cyber Defense and Attack. This paper explores how machine learning can be used in defensive and offensive cyber security, with a concentration on cyber-attacks against machine learning models. It discussed how machine learning can be used to address some cyber-attacks, for example the smart botnets, advanced spear fishing, and evasive malware. Moreover, it clarified how machine learning can be used in computer defense for topics like threat detection and prevention, malware detection and classification, and network risk scoring. [7] Published an article on Unified Computational Modelling for Healthcare Device Security Assessment. The security mechanisms used to manage healthcare systems are analyzed in this article, and a mathematical model is proposed to rate them in order of importance and preference. Thus, it employs the Fuzzy Analytic Network Process (ANP) in combination with the Technical for Order Preference by Similarities to Ideal Solution (TOPSIS) to define appropriate protection mechanisms for preventing trespassing on healthcare equipment. Machine Learning (ML)-based healthcare devices achieved the highest importance of all other protection strategies and security mechanisms, according to the article analysis. [8] Produced a review article on Deep Learning Security and Privacy Defensive Techniques. Deep Learning and deep learning systems are still vulnerable to a variety of security threats and incidents. Thus, it is important to attract the industry's focus to Deep Learning security risks and associated countermeasures methods, therefore, the authors undertake a detailed survey of Deep Learning security and privacy issues and countermeasures in this article. Also, discussed upcoming threats and existing problems. The results show two types of possible security attacks, evasion, and poisoning.

[9] Authors produced a book on Machine Learning and Security. It includes a guide for addressing the combination of Security and Machine Learning as well as a toolkit of machine-learning algorithms that can be used to solve a variety of security issues. It discovers how machine learning has aided the success of today's spam filters, detect threats such as breaches, theft, and impending system failure easily. Moreover, extract valuable information from device binaries to conduct malware detection and discover network attackers by looking for patterns in datasets. Analyze how attackers take advantage of consumer-facing services and software functions. Also, take the machine learning algorithms from the lab to the real world. Finally, recognize the risks that hackers raise to machine learning applications. [10] Produced a survey paper on Machine Learning and Deep Learning Methods for Intrusion Detection Systems. This survey presents an intrusion detection system (IDS) taxonomy that classifies and summarizes machine learning and deep learning-based IDS literature using data objects as the primary dimension. The suggested taxonomic scheme used as a starting point to show how machine learning and deep learning approaches can be used to solve key IDS challenges. The results of this survey show that the lack of available datasets could be the most difficult issue to solve. So, unsupervised learning and incremental learning methods have a lot of potential. Interpretability is critical for functional IDSs. Since interpretable models can convince consumers and help they make decisions.

[11] Provided a survey paper on Data Mining (DM) and Machine Learning (ML) Methods on Cyber Security. This paper provides an overview of how Machine Learning (ML) and Data Mining (DM) approaches have been used to simplify cyber detection systems and explores the necessary areas on cyber security. The paper focused on how machine learning methods have been used in the implementation of cyber security. Support Vector Machine Algorithms, Genetic and Evolutionary Algorithms, Association Rules, and Sequential Patterns are all examples of DM algorithms that show an effective result in supporting Intrusion Detection System. [12] Produced a survey paper on Machine Learning Techniques for Cyber Security in the Last Decade. Through introducing a literature on ML methods for cyber protection, including intrusion, spam, and

malware detection on computer and mobile networks, this paper seeks to offer a detailed review of the difficulties that ML techniques pose in defending cyberspace from threats. It gives a brief overview of machine learning models' implementations in the area of computer defense, focusing on the last ten years' progress. The result shows that each cyber challenge has its own characteristics that make even the most sophisticated machine learning model difficult to contend with. It is difficult to produce a single recommendation based on a single model for all attacks. When choosing a model to detect a cyberattack, different factors including detection rate, time complexity, classification time to find undiscovered and zero-day attacks, also, accuracy of an ML model should be considered.

[13] Proposed a research paper on Cyber Security Fraud Prevention using Data Analytics Developing a Layered Framework with Preconditions to Enable Fraud Identification in Bank Sector. This research concentrated on cybersecurity by using data analysis, especially real-time data analysis, in the banking industry to detect malware intrusions. This paper developed the L-based Malware Detection Framework to classify malware operations in banks by combining multiple analytical models and analyzing data from numerous sources in real-time. Interviews with bank workers are used to test the system that has been established. [14] published a paper that evaluate Machine Learning Algorithms for Detecting DDoS Attack. The chi-square and information gain function selection processes are used to identify the key aspects. Some machine learning models, such as Navies Bayes, C4.5, SVM, KNN, K-means, and Fuzzy c-means clustering, are built to improve the identification of DDoS attacks using the chosen attributes. [15] produced a paper on Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. The effects of machine learning in cybersecurity and CPS/IoT are discussed in this paper. It identifies many advantages (good uses) that machine learning has introduced to security and CPS/IoT, such as better intrusion detection systems and the accuracy of decision in CPS/IoT. More urgently, it examines machine learning (bad use) weaknesses from the viewpoints of security and CPS/IoT, and the ways in which machine learning applications can be hacked, manipulated, and corrupted at every point in the machine learning stages. Finally, the use of machine learning in the implementation of cyberattacks and intrusions is a rising development that is highly worrying (ugly use). Thus, the paper looks at emerging mechanisms that have the potential to enhance target acquisition and current threat trends, specially, those that can allow novel attacks that have not been seen before.

[16] Provided a conference paper on Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture. This paper examines the study of unusual behavior associated with phishing web attacks, as well as how machine learning methods can be used to combat the challenge. This research is conducted using infected data sets and Python software to improve machine learning for detecting phishing attacks via the analysis of URLs to identify if they are correct or incorrect URLs based on attributes of the URLs, with the aim of providing real-time information to take strategic decisions that reduce the effect of an attack. [17] Provided a research paper on Trojan Traffic Detection Based on Machine Learning. This paper examines the network behavior characteristics and network traffic of several popular Trojans, such as Zeus and Weasel, and presents a machine learning-based Trojan traffic identification algorithm. [18] Presented a survey paper on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. It explores current security risks and conducts a comprehensive evaluation of them from two perspectives: training and testing/inferring. Following that, it divides existing machine learning defense strategies into four categories: vulnerability evaluation processes, training phase countermeasures, testing phase countermeasures, data protection, and privacy. The study then goes on to list five noteworthy developments in machine learning technology, including security risks and defensive methods, that are worth further investigation in the future.

Table 1. Summary of previous studies on cybersecurity threats and machine learning soloutions.

Ref.	Published Year	Paper Topic	Cybersecurity Threats	Machine Learning Solutions and Algorithms
[1]	2018	Machine learning and deep learning methods for cybersecurity	DoS, Probe.	Support vector machine, k-nearest neighbour, decision tree, deep belief network, recurrent neural networks, and convolutional neural networks.
[2]	2020	Cybersecurity data science: an overview from machine learning perspective	DoS, DDoS, Probe, Intrusion, Malware.	KNN, Decision tree, SVM, K-means, Clustering, Naïve bayes, Random forests, Association rule, Behaviour rule, generic algorithm, RNN, LSTM.
[3]	2014	Applications of machine learning in cyber security	Phishing, Network Intrusion, Keystroke Dynamics, Breaking Human Interaction Proofs	fuzzy c-means clustering, neural networks, Probabilistic Neural Network (PNN), Genetic Network Programming (GNP), Logistic Regression (LR), Classification and

			(CAPTCHAs), Social Network Spam,	Regression Trees (CART), Bayesian Additive Regression Trees (BART), Support Vector Machines (SVM), Random Forests (RF).
[4]	2017	Machine learning and cyber security	Intrusion, zero-day.	Bayesian Network, Decision trees, Clustering, Artificial Neural Networks (ANN), Genetic algorithm and genetic programming, Hidden Markov Models (HMM), Inductive Learning.
[5]	2018	On the effectiveness of machine and deep learning for cyber security	Intrusion, Malware analysis, Spam and phishing detection.	Naïve Bayes, Logistic Regression, Support Vector Machines, Random Forest, Hidden Markov Models, K-Nearest Neighbour, Shallow Neural Network, Clustering, Association, Fully connected Feedforward Deep Neural Networks, Convolutional Feedforward Deep Neural Networks, Recurrent Deep Neural Networks, Deep Belief Networks, Stacked Auto encoders.
[6]	2018	Machine learning for cyber defence and attack	Unauthorized Access, Evasive Malware, Spear Phishing.	Threat detection and classification, Network risk scoring, automate routine security tasks and optimize human analysis.
[7]	2021	Unified computational modelling for healthcare device security assessment	Unauthorized access.	Analytic Network Process, multiple criteria decisions making,
[8]	2020	A review of deep learning security and privacy defensive techniques	Malware, Adversarial malware attacks, Ransomware, Wi-Fi impersonation, Spam, Download attack, Insider threats.	Feed-Forward Neural Network (FNN), Convolutional Neural Network, Recurrent Neural Network, Generative Adversarial Network.
[9]	2018	Machine learning and security	Malware, worm, Trojan, spyware, adware, ransomware, sniffing, key logger, spam, ATO, phishing, DoS, zero-day.	Artificial Neural networks, ARIMA, Median absolute deviation, one-class Support Vector Machines, Isolation forests, k-Nearest Neighbors (kNN).
[10]	2019	Machine learning and deep learning methods for intrusion detection systems	Misuse, Anomaly, intrusion detection.	ANN, SVM, KNN, Naive bayes, Logistic regression, Decision tree, K-means, DBN, DNN, CNN, RNN, GAN, RBM, Auto encoder.
[11]	2017	Data mining (DM) and machine learning (ML) methods on cyber security	Packet-Level Data, Net Flow Data, Misuse Detection, Anomaly Detection and Hybrid Detection.	ABNN, Association rule, Bayesian network, K-means, Clustering, Naïve bayes, Random forest, HMM, SVM, k-NN.
[12]	2020	Machine learning techniques for cyber security in the last decade	Spam classification, fraud detection, malware detection, phishing, dark web or deep web sites and intrusion detection.	Support vector machine, decision tree, k-nearest neighbour, random forest, naïve bayes, ANN, RNN, Auto encoder.

[13]	2017	Cyber security fraud prevention using data analytics developing a layered framework with preconditions to enable fraud identification in bank sector	Web application attack, Malware, DoS, DDoS, Keylogger, and Behaviour Log Files.	N-grams.
[14]	2011	Machine learning algorithms for detecting DDOS attack	DDoS.	Naive Bayes, K-Mean Clustering, SVM, k-NN Classifier, FCM Clustering.
[15]	2019	Machine learning for security and the internet of things: the good, the bad, and the ugly	Misuse, Anomaly, Malware detection.	Classification, Regression, Dimensionality reduction, Clustering, Density estimation, Policy search, Value function approximation.
[16]	2019	Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture	Phishing.	Decision trees, nearest neighbour learning, Markov models.
[17]	2020	Trojan Traffic Detection Based on Machine Learning	Trojan.	Naive Bayesian algorithm, decision tree, Random Forest.
[18]	2018	A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View	Causative, exploratory, integrity, availability, privacy, targeted, and indiscriminate attacks.	Deep neural networks, support vector machine, Naive Bayes,

3. Research Methodology

The criteria for performing a systematic mapping study were applied in this research. This strategy was chosen for a variety of purposes. It is a method of finding, analyzing, and interpreting all related studies on a specific study topic in a systematic and organized manner. This method contains many phases starting with identifying the research questions, as well as the search criteria. Then, extracting the data and map it to the research questions. Finally, analyze the results [19]. The following research questions formulated and discussed in this research to guide the study:

Research Question 1: What are the possible Machine Learning techniques that could be used for improving Cybersecurity? This question will identify the possible ML techniques and methods that can be used to improve and robust the cybersecurity.

Research Question 2: What are the possible cyber-attacks that can be reduced using Machine Learning techniques? This question will identify the possible cyber-attacks and threats that ML techniques can address to improve the cybersecurity.

Research Question 3: How effective are the various types of Machine Learning techniques in improving the Cybersecurity? This question will identify how ML techniques improve and robust the cybersecurity. Also, it will discuss and highlight different applications of ML in cybersecurity.

4. Analysis and Results

Machine learning approach is based on the human brain's capacity to learn from prior knowledge in real time. Various fields of science have extensively used these methods to solve complex challenges [20]. With the increased use of the internet and a broad range of network technologies, cyber protection is growing rapidly. The results of analyzing previous studies are summarized in classification of cyber-attacks, machine learning algorithms, and application of machine learning in cybersecurity.

4.1 Classification of Cyber Attacks

The target of the attack is the first aspect for classifying it. This is often linked to how an attacker monetizes an attack. Based on [20] this can be classified into six categories as shown in Figure 1, which are: hacking, phishing, malware, data leakage, spam, and DoS attacks. The attack vector is a second aspect for categorizing an attack; it describes the weakness exploited by an attacker to achieve access to a network or computer system to carry out harmful attacks. Attack vectors can be discovered in hardware, network, or application layers.

Figure 1. Categories of Cyber Attacks.

4.2 Machine Learning Algorithms

The main categories of machine learning algorithms are Supervised Learning, Unsupervised Learning, and Reinforcement Learning [9][20]. Each of the main categories contains different machine learning algorithms [14] [20] as shown in Table 2.

Table 2. Machine Learning Algorithms Categories

<table>
<tr><th colspan="7">Machine Learning Algorithms</th></tr>
<tr><th colspan="2">Supervised Learning</th><th colspan="4">Unsupervised Learning</th><th rowspan="2">Reinforcement Learning</th></tr>
<tr><td>Classification</td><td>Regression</td><td rowspan="5">Clustering</td><td rowspan="5">Association</td><td rowspan="5">Hidden Markov Models</td><td rowspan="5">Dimensionality Reduction</td></tr>
<tr><td>Support Vector Machines (SVM)</td><td>Logistic Regression (LR)</td></tr>
<tr><td>Naïve Bayes (NB)</td><td rowspan="2">Random Forest (RF)</td></tr>
<tr><td>K-Nearest Neighbor</td></tr>
</table>

(A) Supervised Learning

When objectives are defended to achieve from a specific collection of inputs, supervised learning is used, often known as a task-driven strategy. The most widely used supervised learning approaches in machine learning are classification and regression approaches. These methods are widely used to identify or forecast the future of a security issue [2] [20]. Most widely classification algorithms used are Support Vector Machines (SVM), Naïve Bayes (NB), and K-Nearest Neighbor. The important regression algorithms are Logistic Regression (LR), and Random Forest (RF) [20].

(B) Unsupervised Learning

The key challenge in unsupervised learning is to search patterns, constructs, or information in unlabeled data, which is known as a data-driven approach [2]. Cyber-attacks, such as ransomware or hidden attacks that modifying their actions rapidly and independently to prevent detection in the field of cybersecurity can be reduced by clustering approaches, which are a form of unsupervised learning, it may succeed in the discovery of hidden patterns and constructs in datasets, allowing for the detection of indications of advanced threats. Clustering methods may also be helpful in finding irregularities, policy breaches, tracking, and removing noisy instances in files [2] [20]. In association approach, the unknown patterns between data are established, and they have been generated in a way that is suitable for prediction functions. They can provide a production of basically invalid rules, so they must be subjected to proper inspections by knowledgeable personality. The Hidden Markov Model (HMM) is a Markov model used in mathematical modeling in which the mechanism being constructed is a Markov method with unobserved variables [20]. The last approach of unsupervised learning is Dimensionality Reduction, which is a method of extracting or approximating the information distribution using mathematical models; it determines the density of information subsets in order to analyze correlations [2] [20].

(C) Reinforcement Learning

Reinforcement Learning is a form of machine learning that is driven by its psychological effects. This learning differs from other algorithms in that it is not given any guidance to accomplish the task; rather, it completes it by itself and learns from past experiences.

4.3 Application of Machine Learning Algorithms in Cybersecurity

This section maps each machine learning algorithm with the corresponding cyber-attack that the algorithm could address and reduce [2] [4]. Table 1 identify each machine learning algorithm and the cyber threat related to that algorithm [2].

1. SVM

It is used to distinguish different types of attacks including DoS, Probe, U2R, and R2L. Also, for detection and classification of intrusion and DDoS attacks. Moreover, it could be used with PSO or KNN to create and establish an intrusion detection system, and with FCM clustering and ANN to establish system for detecting network intrusion [2] [4] [8].

2. KNN

It is used to establish system for detecting network intrusion. Also, reduction of false alarm. Moreover, it could be used with K-Means or Clustering to establish a system for detecting intrusions. And used with Decision Tree to establish system for anomaly intrusion detection [2].

3. Naive Bayes

It is used to establish a system to detect intrusions in multi-class classifications [2] [9].

4. Decision Tree

Through running malicious software on a VM and analyzing the behavior information for intrusion detection, it is possible to identify suspicious code's behavior information. Moreover, it is used for the construction of an efficient network intrusion

detection system. It can be used with Generic Algorithm to address the limited disjunction issue in an intrusion detection system that based on decision tree, and with ANN to assess the effectiveness of an intrusion detection system [2] [9] [10].

5. Random Forest

It is used to establish system for detecting network intrusion [2] [10].

6. Association Rule

It is used to establish system for detecting network intrusion [2] [10].

7. Behavior Rule

To develop an intruder prevention system for mission-critical medical cyber physical applications [10][12].

8. Supervised

It is used to analyze and detect malwares [2] [10].

9. Hidden Markov Models

It is used to establish system for intrusion detection [2] [12].

10. Generic Algorithm

It is used for cyber-terrorist prevention using complex and changing intrusion detection [2] [10].

4.4 Effectiveness of Machine Learning in Cybersecurity Layers

Machine learning algorithms application are effective in reducing and preventing cyber-attacks in hardware, network, or application layers based on previous analysis of algorithms and attacks. This percentages are shown in Figure 2.

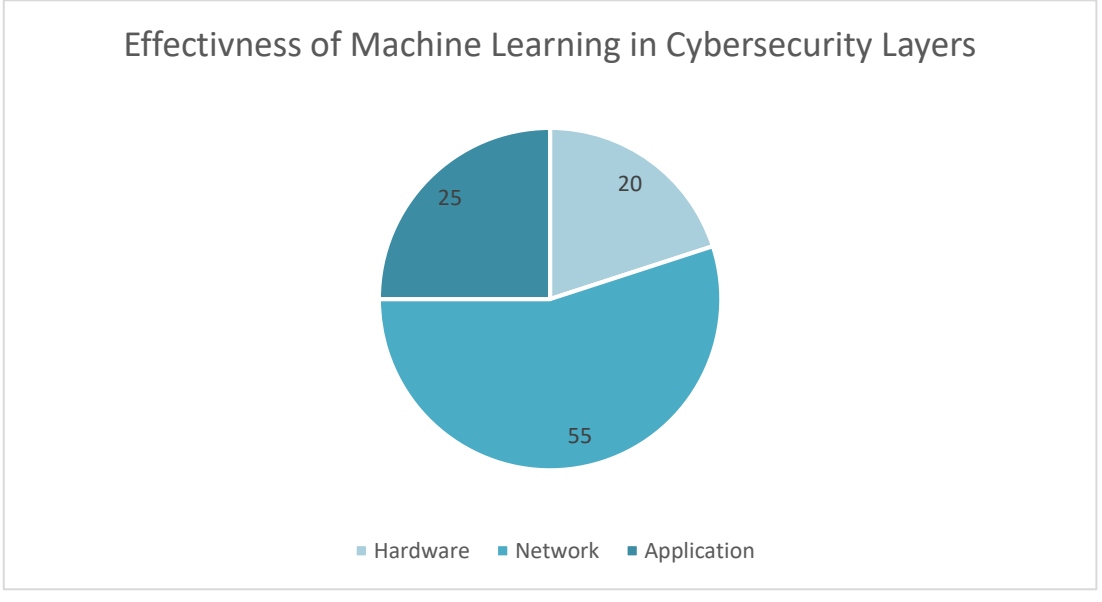


Figure 2. Effectiveness of machine learning

5. Conclusion

Machine Learning (ML) is a subset of artificial intelligence that is closely linked to computational statistics, data mining and analytics, and data science, with an emphasis on teaching machine to learn from data. Its models are made up of a series of laws, processes, or complicated "transfer functions" that is used to find meaningful data patterns as well as predict actions, and that is useful in the field of cybersecurity. Cybersecurity is experiencing major changes in technology and its operations, and data science (DS) is driving the transition where ML, a key component of "Artificial Intelligence," is taking an important role in discovering data insights. After reviewing previous studies and analyzing the results, the results show that machine learning are positively change the cybersecurity field. By mapping major machine learning algorithms with cyber-attacks and discuss the effectiveness of each algorithm for corresponding attack.

Conflicts Of Interest

The author declares no conflicts of interest.

Funding

No funding.

Acknowledgment

I am very grateful because I completed this paper with a lot of support and help of many individuals. First, thanks to my parents for giving encouragement, support, invaluable help, and wholeheartedness. Second, I would like to thank Dr. Mohammed Amin Almaiah who encourage and advise me in completing this paper in proper way.

References

[1] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEe Access*, *7*, 82721-82743.

[2] Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE internet of things journal*, *6*(5), 8076-8094.

[3] Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *Ieee Access*, *7*, 156237-156271.

[4] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

[5] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*, 1-27.

[6] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.

[7] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

[8] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.

[9] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.

[10] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet of Things Journal*, *7*(4), 3559-3570.

[11] Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, *23*(2), 1020-1047.

[12] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881-888.

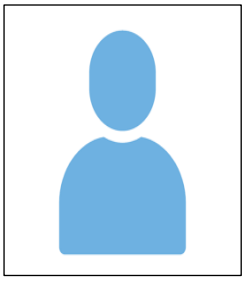
[13] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41-70.

[14] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A survey on blockchain for industrial internet of things. *Alexandria Engineering Journal*, *61*(8), 6001-6022.

[15] Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517-10553.

[16] Sharma, P., Jain, S., Gupta, S., & Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, 102685.

[17] Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Computational Intelligence and Neuroscience*, *2023*(1), 8981988.
[18] Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, *151*, 107198.
[19] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, *169*, 102763.
[20] Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics*, *45*, 101283.
[21] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, 101728.
[22] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, *160*, 165-191.
[23] Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, *176*, 102917.
[24] Zhu, Q., Loke, S. W., Trujillo-Rasua, R., Jiang, F., & Xiang, Y. (2019). Applications of distributed ledger technologies to the internet of things: A survey. *ACM computing surveys (CSUR)*, *52*(6), 1-34.



Aseel Alshuaibi received his M.Sc. degree in Cybersecurity from the King Faisal University (KFU), Saudi Arabia. She has published several papers in well reputed journals and conferences. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic
.

Dr. Mohammed Almaayah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Aitizaz Ali received the master's degree in computer systems engineering (with distinction) from GIK Institute, Topi, Khyber Pakhtunkhwa, Pakistan, and the Ph.D. degree in cybersecurity and blockchain technology from the School of IT, Monash University Malaysia, Jaya, Malaysia. He is a Lecturer with the School of IT, UNITAR International University, Petaling Jaya, Malaysia. He is the author of several Journal papers and international Conferences. He has authored or coauthored more than 20 research papers, including in high-quality journals. His research interests include blockchain, cloud Ccomputing, cybersecurity, cryptography, deep learning, AI, and healthcare systems. moreover. He was the Reviewer of IEEE Internet of Things Journal, IEEE Transactions on Network Science and Engineering, IEEE Access, IET, and Human-centric Computing and Information Sciences Journals for several years.