Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 4291-4307
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.2930
© 2024 by the authors; licensee Learning Gate

Leveraging Machine Learning for Cybersecurity: Techniques, Challenges, and Future Directions

Mohammad Rakibul Islam Bhuiyan[1], Mahfujur Rahman Faraji[2], Mst. Nowshin Tabassum[3], Provakar Ghose[4], Sukanta Sarbabidya[5], Riva Akter[6*]

[1]Department of Management Information Systems, Begum Rokeya University, Rangpur, Rangpur-5404, Bangladesh; rakib@mis.brur.ac.bd (M.R.I.B.).
[2]Master of Science in Engineering Management, Department of Engineering Management, Westcliff University, Irvine, California, United States of America; m.faraji.214@westcliff.edu (M.R.F.).
[3,6*]Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur., Rangpur-5404, Rangpur, Bangladesh; nowshin.mouly@gmail.com (M.N.T.) rivaa350@gmail.com (R.A.).
[4]MS in Business Analytics, University of New Haven, West Haven, Connecticut, United States; pghos1@unh.newhaven.edu (P.G.).
[5]MS in Economics, Purdue University, West Lafayette, Indiana, United States; ssarbabi@purdue.edu (S.S.).

Abstract: This study aims to explore the application of machine learning (ML) in enhancing cybersecurity measures, focusing specifically on intrusion detection, malware detection, fraud detection, and anomaly detection systems. A systematic review of 743 scholarly papers was conducted, from which 115 were selected for in-depth analysis. The review process involved evaluating advancements in ML techniques within the context of cybersecurity. The findings reveal that ML-driven systems significantly enhance the automation of security processes, improve the recognition of novel threats, and reduce human error in cyber threat management. However, challenges such as adversarial attacks and the need for high-quality model training pose significant barriers to the broader adoption of ML in cybersecurity. The study discusses the implications of these findings, emphasizing the necessity for developing robust and adaptive ML models that can withstand adversarial threats while improving integration across various cybersecurity applications. The insights gained from this research provide a comprehensive overview of the potential benefits and challenges of implementing ML in cybersecurity, highlighting the need for continuous innovation in threat detection mechanisms. This review acknowledges limitations such as the predominance of literature from Western contexts, potentially overlooking insights from other regions. Furthermore, the complexity of implementing ML systems in dynamic cyber environments remains a critical challenge. Future research should concentrate on refining ML algorithms to enhance resilience against adversarial threats, exploring the integration of emerging technologies for improved cybersecurity, and addressing gaps in the existing literature regarding the life cycle of ML models in real-world applications.

Keywords: *Cyber threat detection, Cybersecurity, Data security, Information security, Machine learning, Malware detection, Systematic review.*

1. Introduction

According to Niknami & Wu (2024), ML is a part of Artificial Intelligence (AI), it is a system to learn from huge amount of data, detect the threats and take an intelligent decision. ML has become progressively popular and at present used in various field like computer vision, social media platform, mobile networks and cybersecurity and it provides a promising solution in information security (Anzum et al., 2024). The research gap of this topic is that lack focus on predictive behaviors in evaluations of ML model and also no study has considered all ML software and hardware life cycle stages. Another gap is that detection of phishing website attacks in information security solving by ml (Dasari & Samanta, 2024).

According to Jo (2020), ML algorithms are gradually more effective in certain scheme. Machine

* Correspondence: rivaa350@gmail.com

learning (ML) algorithms can be considered into four types: supervised, unsupervised, semi- supervised and reinforcement learning. Supervised learning algorithms use labeled training data to make predict outcomes or make decisions. In information security, supervised learning is especially valuable as it can be trained to identify patterns linked to both legitimate and malicious activities (Liu et al., 2024). Unsupervised learning algorithms aim to uncover hidden patterns or inherent structures in data without using predefined labels. In information security, unsupervised learning is particularly valuable for anomaly detection where the aim is to identify unusual patterns that might indicate malicious activity or other security incidents. Semi- supervised learning algorithms leverage both labeled and unlabeled data to improve learning precision, allowing models to use a small amount of labeled data along with a larger pool of unlabeled data to enhance the learning process (Lyubchyk, & Yamkovyi, 2022).

Bhuiyan et al., (2024) stated that Machine Learning (ML) is now widely available and accessible to organizations of all sizes. ML applications serve purposes that were unimaginable just a few years ago. From the perspectives of system security, privacy and public safety, ml introduces both opportunities and challenges for various applications. This review paper mainly focuses on the study of data security using machine learning technologies. We are also describing how ml algorithms can be applied in information security and ml techniques and challenges also addressed (Nanath, & Rahman, 2022).

Kaigorodtsev & Kaigorodtseva (2020) In the digitalization era, technology became essential across all sectors, offering numerous conveniences and accessibilities. However, it also introduced several problems, such as privacy concern, security vulnerabilities, and the potential for misuse. Balancing these benefits and challenges is crucial for the responsible use of technology. Ensuring the security was very robust for the systems developer because the attackers were developing progressively. Every digital process and social platform engendered gigantic data. Attack strategies are rapidly evolving to bypass generic signature-based defenses, similar to advancements in web and mobile technologies (Hossain et al., 2024). ML techniques offered promising solutions due to their ability to adapt quickly to new and unknown situations, making them suitable for addressing these complex challenges. A variety of securities issues were being used in ML techniques (Gupta et al., 2023).

According to Rahman et al. (2024), An excessively limited focus on assessing ML models based only on decontextualized predictive behaviors, ignoring other essential model properties, was one of the major research gaps in the field of machine learning. Furthermore, there needed to be a stronger focus on finding zero-hour or freshly created phishing website attacks, which necessitated more study and implementation of machine learning and deep learning methods (Bhuiyan et al., 2023). Furthermore, a comprehensive overview of the variables influencing the greenhouse gas (GHG) emissions generated by ML models was lacking, as were the decisions made regarding hardware and software design (Park & Kim, 2023). Milon et al. (2024) stated that there was a lack of research on machine learning's unintended effects on user autonomy and hardware lifetime (Bhuiyan et al., 2024). The different actors in ML Ops also frequently communicated with one another too late in the solution design process and lacked synchronization. The communication gap between domain experts and AI experts was a frequent problem (Meng, 2024).

Again, Meng (2024) in terms of challenges, researchers had typically talked about them to inspire more research as opposed to providing concrete answers. While some difficulties were unique to particular sites or datasets, others showed up during model implementation. Only a few of the typical difficulties were discussed (Kostaki & Karayianni, 2021). Zhou & Zou (2023) even in the absence of complete explain ability, transparency in the model development and validation processes including the clear reporting of model uncertainties were essential to creating trustworthiness (Bhuiyan, 2023). Furthermore, substantial resources were frequently needed for training, internet access, software, and other computational and technical necessities, as well as for collecting and using big data and machine learning. Nevertheless, this was primarily accurate in a limited number of worldwide locations. To support comparable research efforts, other regions needed better infrastructure and better access to resources, as indicated by the fact that most of the studies in this review were from Western Europe and China (Chi et al., 2023). Based on the research gaps, the following research objectives are given below:

RO1: To define our study's scope by researching a machine learning-based, dynamically enhanced, automated, and advanced security system.

RO2: To offer a thorough understanding of machine learning algorithms that are helpful for intelligent data automation and analysis in cybersecurity.

RO3: To examine the barriers that must be overcome to fully apply machine learning techniques for increasing security and efficiency.

2. Literature Review

Faraji et al. (2024) conducted this literature review, which studied the existing research, theories, and thesis papers on machine learning (ML) in information security. this paper represented how ML was used for security, the applications of algorithms in machines, and discussed the advantages and ideas related to these applications.

2.1. Machine Learning

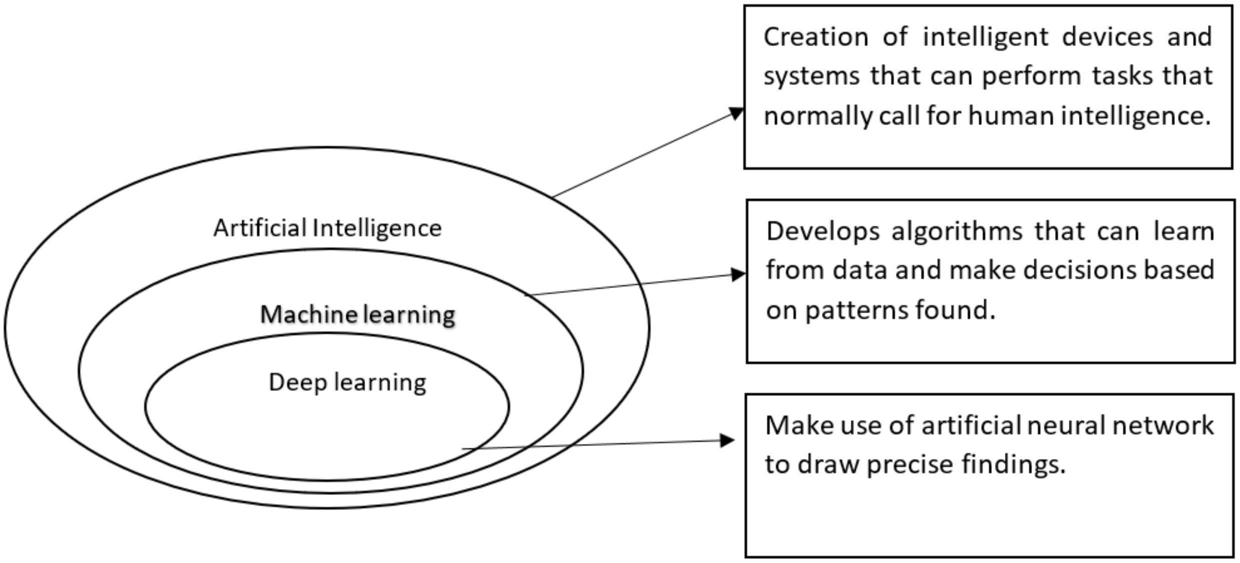
Artificial Intelligence
Machine learning
Deep learning
Creation of intelligent devices and systems that can perform tasks that normally call for human intelligence.
Develops algorithms that can learn from data and make decisions based on patterns found.
Make use of artificial neural network to draw precise findings.

Figure 1.
ML in cybersecurity.

According to Bhuiyan et al. (2024), The scheme of ML formed a conclusive model which indicated the data. the algorithms of ML inquired in many enclosures, functioning as fraud detection, credit assessment, speech and image recognition, and neural networks. It Generated a significant advancement, extension buried of healthcare, finance, transportation and more unlocked up to date for research and innovation alongside ML. machine learning (ML) has numerous robust and statistical tactics for predictive motives, algorithms in general were supervised and unsupervised learning (Wang et al., 2023). Cracking unremarkable current troubles, network security was an altering sphere. Cyberattacks alluded to abusive ventures that quarried electronic information systems, networks and skeletons. their intension was to thieve, revise, destroy information.

ML engineers operated exploratory data analysis in order to extract meaningful insights from their data (Niknami & Wu, 2024). They could use it to develop models that appropriately reflected their data and made well informed judgments (Pasrija et al., 2024). about it. ML techniques played a vital role in intrusion detection systems, malware detection, phishing detection, decision trees, Bayesian approaches, artificial neural networks were the grouping of ML algorithms. The information security in ML was mostly disposable for the industrial sector, networking systems, and electronic transactions (Niknami & Wu, 2024). ML became more accessible, leading to its use in various new applications. Machine learning (ML) presents both opportunities and challenges in the realms of cybersecurity, privacy and public safety. While it can improve privacy and security measures, it also brings risks such as opaque decision making, biased algorithms and safety vulnerabilities, which complicate traditional privacy protection

DOI: 10.55214/25768484.v8i6.2930

methods. (Bertino et al., 2023).

2.2. ML in Information Security

According to Milon et al. (2024), ML in information security employed algorithms and models that acquire knowledge from data from to detect, examine, and counteract cyber threats. Information security was essential as it safeguarded sensitive data, systems and networks from unauthorized access, breaches and various threats. Automation has become more crucial for security teams as cyber threats grow in complexity prevalence. common hazards included malware, phishing, ransomware, Dos, and zero-day attacks. Traditional defense measures were often flawed, and many detection methods still depend on manual analysis, making it difficult to identify advanced threats (Padole et al., 2024). However, ML, ml surpassed human capabilities in recognizing patterns and making security decisions. As a result, intelligent decision-making using ML for automation has become a viable solution to meet the security demands of dynamic network systems (A & P M, 2023).

2.3. Intrusion Detection Systems

Niknami & Wu (2024) stated that in computer security systems, intrusion detection systems were a verified clarification for monitoring events. They used machine learning (ML) to expose the latest types of attacks and abnormalities, with the model using a tree-based approach alongside these crucial attributes. Adversarial ML, where attackers manipulated ML models, was a major concern, requiring ongoing research and innovation to keep ML based security solutions robust against evolving cyber threats. Data persistence was crucial for software systems, with data privacy being vital throughout the lifecycle of modern systems. Security needed to both cover hardware and software aspects, but ML introduced unique challenges, particularly in managing data quality due to model uncertainty. Ensuring data quality was essential for protecting ML based systems from data-oriented attacks, both during design and runtime (Singhal, 2024).

2.4. Threat detection

In designing the information security, cyber defense mechanisms encompassed a variety of strategies, technologies and practices (Islam & Bhuiyan, 2022). Advanced threat detection was one of them. With the rapid advancement of technology and the increasing reliance on digital systems, advanced threat detection and defense mechanisms became necessary to identify, mitigate, and respond to these evolving threats effectively. through this, vulnerabilities were discovered (Rose et al., 2022). The evolution of security mechanisms, particularly in the context of threat detection, progressed. Initially, threat detection machines relied on manually defined rules and elements. However, with advancement in data analytics, these systems increasingly have adopted ML techniques (Pasrija et al., 2024).

2.5. Malware detection

Hossain et al. (2024) it was shown that machine learning is highly efficient in detecting cyber security threats, allowing systems to process extensive datasets, recognize patterns, and identify anomalies that indicated possible risks. By examining the traits of existing malware, machine learning algorithms were capable of recognizing recurring patterns and developing models to detect new, unfamiliar malware based on these resemblances. A deep learning-based malware detection approach consisted of three main stages: first, gathering and analyzing malware samples with dynamic analysis tools to capture execution traces. Second, using these traces to define malware behaviors and extract relevant features and finally employing a deep learning model to differentiate between benign and malicious software. ML techniques were effective in identifying polymorphic and new attacks, potentially surpassing conventional detection methods in the future.it emphasized the importance of cost- effective training methods for malware detection and the need for malware analysts to achieve an expert level understanding of ml- based detection techniques (Mihalache et al., 2024). Mihalache et al. (2024) further explained that malware detection involved two types of analysis: static and dynamic. static analysis detected malware by examining a file without executing it, while dynamic analysis observed the behavior of software during execution, typically in a controlled environment.

2.6. Anomaly Detection

According to Parhizkari (2024), Anomaly detection had been a long - standing research topic, with various techniques developed over the years. the main challenge was identifying patterns in data that deviated from expected behavior. Anomaly detection was used in multiple applications, including cyber security, network intrusion detection, unusual video activity, fraud detection, streaming and hyperspectral imaging (Molla et al., 2023). While traditional statistical methods for anomaly detection had lost popularity, ML has become increasingly chosen for this purpose (Bhuiyan et al., 2023). ML models could identify deviations from normal behavior and continuously monitor network traffic and system logs, comparing incoming data against the learned patterns (Fung et al., 2024).

2.7. ML in Fraud Detection

From the perspective of Garai et al. (2023), ML has emerged as a powerful tool on fraud detection, offered various advantages that significantly enhanced an organizations ability to combat fraudulent activities.

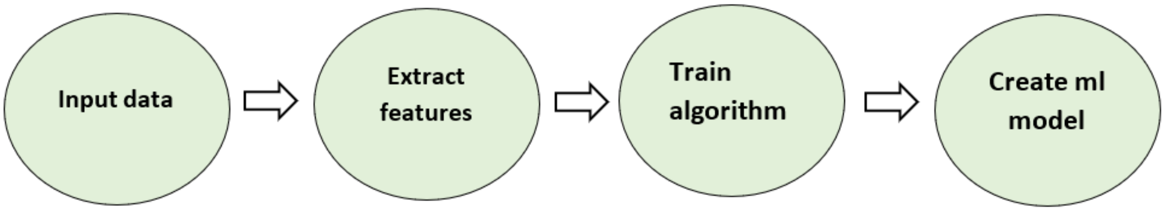

Figure 2.
ML in fraud detection.

ML models can swiftly and accurately process large volumes of data, detecting pattern and anomalies that may signal fraudulent behavior (Bhuiyan & Akter, 2024). They functioned in real time, enabling the instant detection and prevention of deceitful transaction. This was particularly valuable in financial transactions, where quick response times were crucial. Fraudsters constantly developed new tactics and adapted to countermeasures, but ML models were effective in combating this by learning from historical data and quickly adjusted their detection strategies. This enabled them to identify new fraud patterns and adapt without manual intervention, keeping organizations ahead of fraudsters (Boulsane & Afdel, 2024).

ML was the science of developing and applying algorithms capable of learning from historical data. It proved to be an ideal solution for information security. According to the authorized access order, ml could use its model to estimate the unauthorized access and reject it. the traditional fraud detection model was based on a static rule-based system, but ml worked as a dynamic model. The ml model was effective for decision making and also secured the information systems (Abitova & Abalkanov, 2024).

3. Methodology

Watanabe et al. (2023) aimed to outline the researchers' goal and objectives of the review papers, with the suitable title of the paper being "machine learning in information security". the study's focus was on the different kinds of machine learning like as, how they connect to information security systems and how to detect fraud. With the recent developments of information security systems, the author included the systematic review process how ml coped with information security. In the literature review the author additionally expressed the applications of the ml such as intrusion detection systems, threat detection, malware detection, anomaly detection (Niknami & Wu, 2024). The primary goals of this paper were to identify gaps in the literature and weed out research that weren't relevant.

The screening procedures utilized in the preceding stage and systematic literature review are the same in order to guarantee coherence and consistency. To conduct bibliometric analyses, authors retrieved papers from databases such as Scopus, Web of Science (WOS), and Google Scholar (Robledo et al., 2021). Through the use of bibliometric methodologies, which developed the conceptual and

DOI: 10.55214/25768484.v8i6.2930

intellectual framework that enabled authors to deduce meanings through co-word, co-citation, and co-authorship analysis, the extracted documents from any of the aforementioned sources are examined. The research impact of the published papers was determined using a variety of bibliometric indices, including citation counts by paper, author and institution and nation (Rahman et al., 2024).

According to Yeldho et al. (2024), The study on machine learning in the context of information security emerged in the research area, nearly every item being released between 2020 to 2024. Because of this, the screening procedure focused on quality as opposed to quantity. The Scopus, Web of Science, Google Scholar and other searches comprised the following keywords: "machine learning ", "machine learning algorithms", "information security", "threat detection", fraud detection. The only works considered were Peer-reviewed studies in the fields of artificial intelligence, machine learning, and data science. (Sundaram Nanhay Singh, 2023). The search yielded titles, keywords, citations, abstracts, and all other relevant research information. The authors located 2441 papers using the given keywords, of these, they determined 743 papers that meet the study's eligibility requirements (Pearson, 2024). the topic matter was restricted to data science, information security, machine learning, artificial intelligence, and machine learning techniques and applications, bringing the total to 743 publications. Thus, review-based qualitative research was not included in the study (Divya et al., 2023). 115 studies remained finally after 228 were eliminated. Following the processes of data inclusion, exclusion, and segmentation, the author read through the literature on threat detection, machine learning and information security (Milon et al., 2024).

From the perspective of Haddaway, (2022), The author conducted a manual search for the document. The author started by conducting a google scholar search using two or more keywords related to the body of current literature. Second, the writers reviewed the included articles reference list. For the articles included in the third stage, the author used a citation tracking system. Citation tracking systems were typically accessible through indexing services like the Scopus and the web of science. When an article was manually searched, the research engines returned appropriate results based on the user's search query title (Faraji et al., 2024). Following data collection, the author creates themes and cultures using a variety of bibliometric research methods that were based on machine - generated algorithms. Selecting the proper ml applications for specific problems was challenging and also related to the proper techniques. Nevertheless, the use of ml in preventative defence systems in cybersecurity (Dhibar & Maji, 2023).

Ml contributed to a more intelligent, adaptive and efficient defence posture. The purpose, benefits, and limitations of machine learning in information security are discussed in this article along with its current applications (Kumari et al., 2023). Real time data analysts used ml for quicker threat detection and response. the primary research gap in the field of machine learning was the absence of evaluation in real world settings, design and development with specific use cases and well stated explain ability goals in mind. Based on the research gap, the authors analyzed how can ml approaches be fully implemented to improve security and efficiency (Raj & Saundharya Thejaswini, 2022).

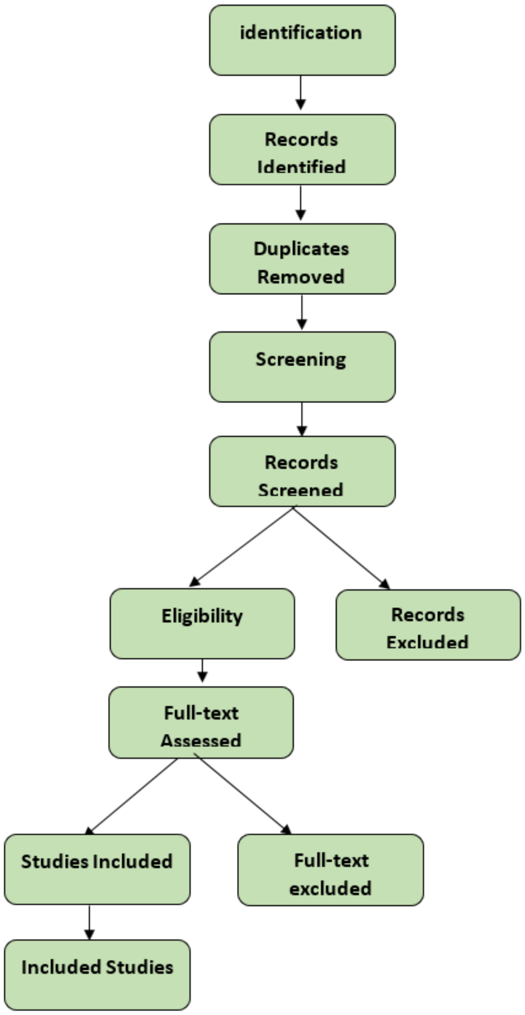

Figure 3.
Methodology.

Rai et al. (2024) subsequently declared that in order to safeguards their networks and data, individual and organizations needed to give priority to their security systems. This meant investing in cutting edge technologies like artificial intelligence and machine learning as well as putting robust security and protections in place. This study served as a guide for the researchers as they highlighted the role, methods and significance of ml in information security space (Bhuiyan et al., 2024). This approach guaranteed that the review paper is detailed, transparent, and repeatable, offering insightful information about machine learning in information security.

4. Discussion

4.1. Introduction to Machine Learning

Azoff (2024) the capability of a machine to mimic human intelligence is the definition of machine learning, an area of artificial intelligence. AI systems are used to complete difficult tasks in a method that is similar to how people would solve issues. Supervised, unsupervised, and reinforcement learning are the three subcategories of machine learning. Results from using machine learning (ML) for trust assessment can be very accurate, particularly when processing large datasets (Islam et al., 2024). The rich data sources that big data provides are the source of this accuracy (Hooda, 2024). However, because of the complexity of the data structures and the large amounts of data involved, traditional methods for evaluating trust in social networks and other large-scale networking environments frequently yield inaccurate results. However, using machine learning (ML) as the main method for managing and interpreting large amounts of data has several benefits (Ammannamma & Vandana, 2023). The researchers have identified three functions that a machine learning system can perform: descriptively, which involves using data to explain past events; predictively, which involves forecasting future outcomes based on data; and prescriptively, which suggests the best course of action based on the data (Son et al., 2022).

4.2. How Does Machine Learning Work?

According to Abu Dabous et al. (2024), A training dataset is utilized by machine learning algorithms to construct a model. Applying the constructed model, the trained algorithm makes predictions when it is given fresh input data.

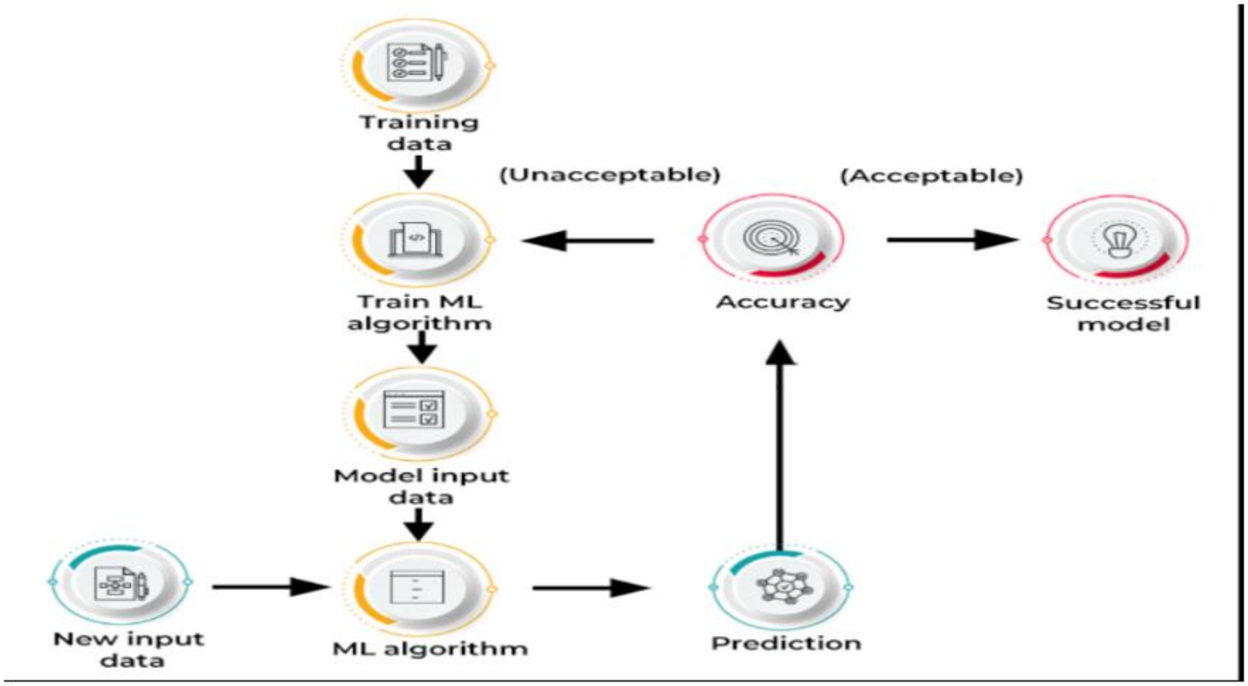

Figure 4.
Working process of machine learning.

4.3. Application of ML

Machine learning is being used by businesses to improve decision-making, increase productivity, identify illnesses, forecast the weather, and do a host of other tasks. The exponential growth of technology demands that we not only prepare for the data we will encounter in the future but also develop more sophisticated tools for analyzing the data we currently have (Reed & Macalla, 2022). We need to create intelligent machines in order to accomplish this goal. While simple tasks can be programmed into machines, it is frequently difficult to directly integrate intelligence into them. Developing a system that lets machines learn on their own is the most efficient course of action. When a machine is capable of learning from input, it takes care of our difficult jobs (Ringel, 2023). Figure 5 demonstrates how machine learning is revolutionizing network security in a major way. These cutting-edge systems make use of complex algorithms to track network activity, quickly spot anomalies, and instantly identify possible threats in real-time (Amin et al., 2024).

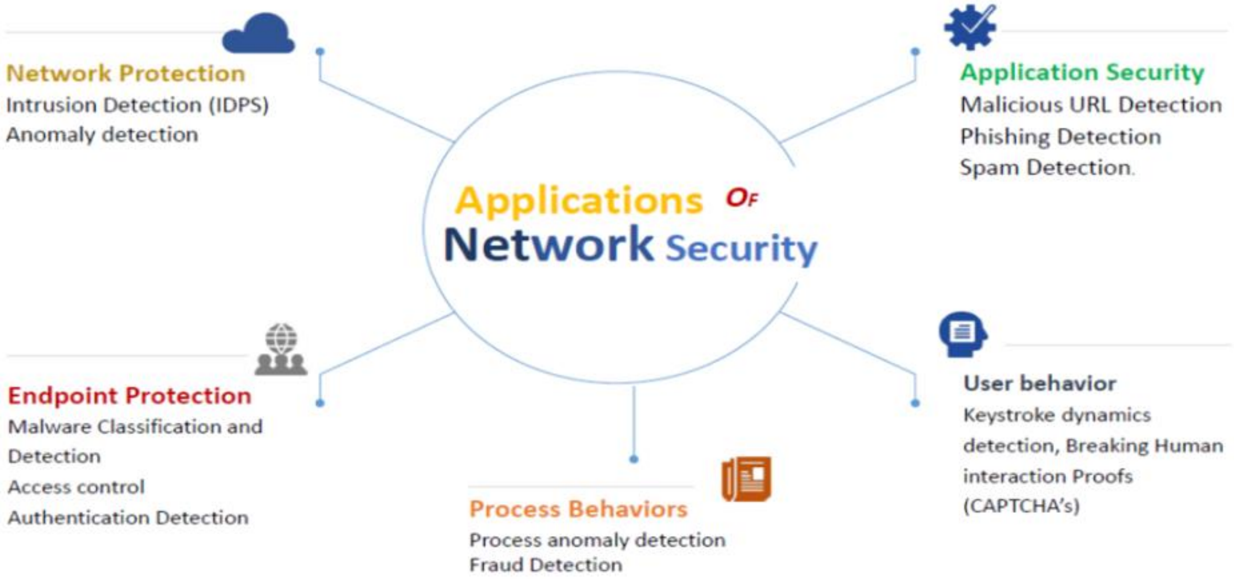

Figure 5.
Network security application of machine learning.

By analyzing historical data, machine learning models can adapt to the constantly changing landscape of cyber threats, which increases the efficiency of intrusion detection and prevention (Gonaygunta, 2023). It's interesting to note that the difficulties in identifying false information in mobile health texts are similar to those in adversarial machine learning for network security (Uddin et al., 2024).

Machine learning-based security systems may benefit from new approaches to thwarting adversarial attacks, such as those outlined in the discussion of a self-reconfigurable system for misinformation detection in (Paya, 2024). Moreover, these programs are especially good at identifying patterns linked to malicious activity, enabling preventative defenses. Machine learning makes network security infrastructures more resilient and adaptable by detecting anomalous network traffic and possible vulnerabilities. Incorporating machine learning into network security not only strengthens defenses against cyberattacks but also provides a scalable and intelligent approach to safeguarding digital assets (Joshi & Oza, 2024).

4.4. Types of Machine Learning

From the perspective of Mire et al. (2021), the field of cybersecurity involves extensive use of machine learning (ML) techniques. These techniques include probabilistic models, decision trees, dimensionality reduction algorithms, regression, boosting, and bagging, as well as distance-based learning (Figure 6). These machine-learning techniques are essential for assessing data breaches and pinpointing weak points in computer networks and systems. The primary advantage of these methods is their ability to swiftly analyze enormous quantity of data and adjust without the assistance of subject matter experts (Sabarmathi & Chinnaiyan, 2021). To further improve network performance and significantly improve threat detection accuracy, machine learning techniques utilize heuristic approaches. Identifying malware, spam, fraud, anomalies, Distributed Denial of Service (DDoS) attacks, and vulnerabilities are just a few of the digital domains where machine learning techniques are put to use (Varma et al., 2024). The four main categories into which machine learning techniques can be classified are supervised, unsupervised, semi-supervised, and reinforcement learning (Figure 6). Every category has a distinct function in tackling cybersecurity issues (Bhuiyan et al., 2024). For instance, unsupervised algorithms are used to cluster unlabeled data and lower feature dimensionality, while supervised learning is used to grow datasets and generate predictions based on them. Semi-supervised learning approaches incorporate aspects of both unsupervised and supervised learning. Finally, reinforcement learning teaches machine learning models to interact with their surroundings to learn and improve various skills (Jo, 2020).

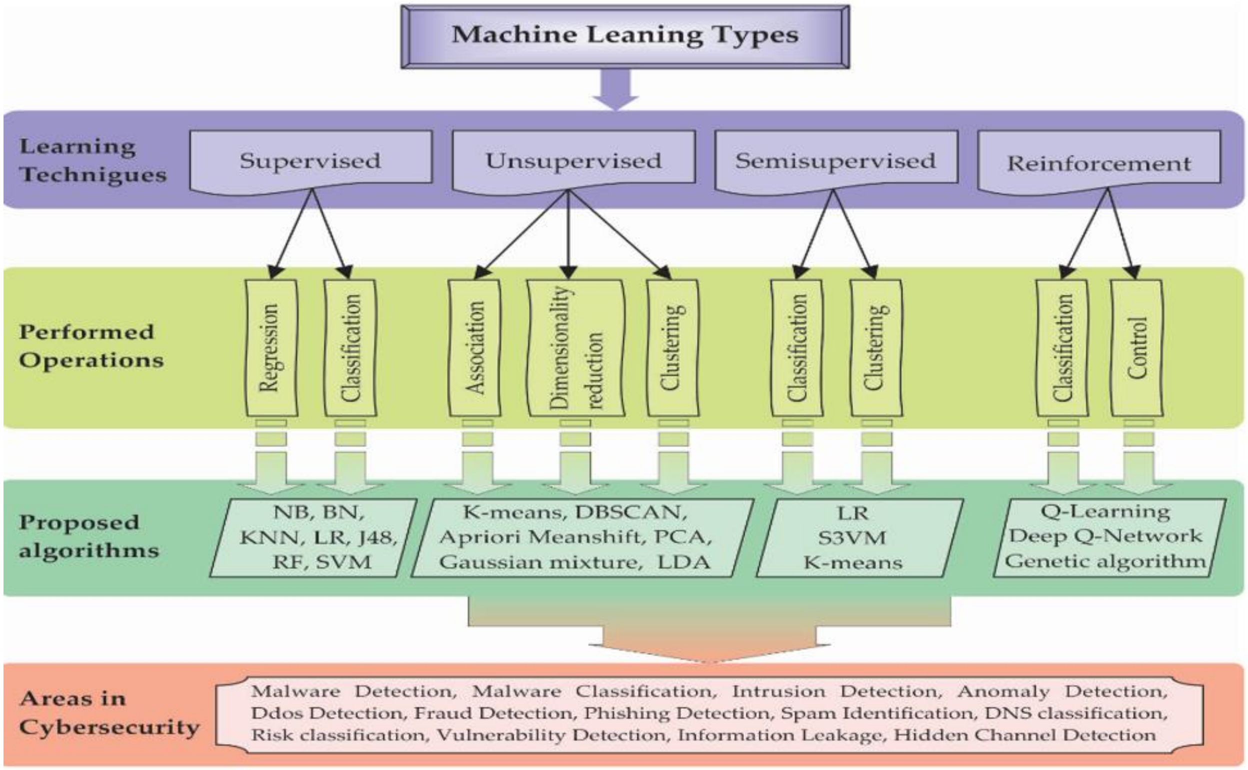
Machine Leaning Types
Learning Technigues
Supervised
Unsupervised
Semisupervised
Reinforcement
Performed Operations
Regression
Classification
Association
Dimensionality reduction
Clustering
Classification
Clustering
Classification
Control
Proposed algorithms
NB, BN, KNN, LR, J48, RF, SVM
K-means, DBSCAN, Apriori Meanshift, PCA, Gaussian mixture, LDA
LR S3VM K-means
Q-Learning Deep Q-Network Genetic algorithm
Areas in Cybersecurity
Malware Detection, Malware Classification, Intrusion Detection, Anomaly Detection, Ddos Detection, Fraud Detection, Phishing Detection, Spam Identification, DNS classification, Risk classification, Vulnerability Detection, Information Leakage, Hidden Channel Detection

Figure 6.
An overview of machine learning techniques used in cybersecurity.

4.5. Challenges and Opportunities of Machine Learning

According to Hossain et al. 2024**,** These days, machine learning is having a big impact on a lot of different industries thanks to its many applications. It influences various activities and processes and is involved in many aspects of our daily lives.

Table 1.
Prospective opportunities of machine learning usages.

Opportunities	**Description**	**References**
Medical diagnosis and treatment	Prognostic and diagnostic problems in medicine and healthcare are addressed by machine learning. Disease detection, patient monitoring and management, medical data analysis, and handling of erroneous medical data are just a few of the areas in which it finds application. These are but a few instances of the uses of artificial intelligence in the medical field.	(Daphin Lilda & Jayaparvathy, 2023)
Compute forecasts	By using algorithms to find the most efficient routes with the least amount of traffic, estimate arrival times, identify pick-up locations, and find the quickest routes to destinations, machine learning improves platforms that use maps and routing. This ensures that users arrive on time.	(Abdul et al., 2023)
Public security	By assisting in the better prevention, reduction, and handling of criminal activity, machine learning can improve community	(Özaşçılar

	safety.	et al., 2024)
Intelligent helpers	Smart assistants, like Siri, Alexa, and Google Assistant, are widely used in daily life to carry out different tasks	(Yang et al., 2021)
Internet Safety	Applications that monitor transactions and differentiate between authentic and fraudulent activity, such as PayPal and GPay, use machine learning. By assisting in the prevention of online financial fraud, this application of machine learning strengthens cybersecurity.	(Milon, 2024; Pan, 2024)
Industry and policymaking in the government	With the aid of machine learning, authorities can more effectively manage and evaluate the vast volumes of data generated by public monitoring devices. Law enforcement organizations can find missing children and capture criminals more quickly when they can analyze anomalies and potential threats in real time.	(Pinsky & Piranavakumar, 2024)

4.6. Challenges of Machine Learning

Indeed, data-driven decision-making enabled by machine learning (ML) has revolutionized several industries (Bhuiyan et al., 2024). Still, it's critical to acknowledge the real-world obstacles that professionals face when learning machine learning and creating applications from the ground up. This study will examine typical problems in the field of ML while giving a balanced, realistic view of these difficulties (Liu, 2023).

Table 2.
Prospective challenges of using machine learning.

Challenges	**Description**	**Reference**
Low data quality	Since noisy, erroneous, and incomplete data can seriously impair classification accuracy and overall results, data quality is an ongoing challenge.	(Qin, 2024)
Unrepresentative training information	A major factor influencing how well machine learning models can generalize is how representative the training data is. A model may produce predictions that are less accurate and show bias against specific classes or groups if the training data does not include all relevant scenarios. Prediction accuracy is increased and biases are lessened when representative data is used in training.	(Mani, 2024; Hocking, 2023)
Surveillance and upkeep	To keep ML models effective, regular maintenance and monitoring are essential. Code modifications and resource updates might be necessary when data or user expectations change, underscoring the significance of constant watchfulness.	(Kilpatrick, 2024)
Receiving unsatisfactory advice	Due to data drift, machine learning models that are used in a particular context may occasionally provide recommendations that are out of date or unrelated. To solve this problem and make sure that recommendations stay in line with what users are expecting today, regular data updates and monitoring are imperative.	(Rashed et al., 2024: Jain, 2022)
Insufficient expert resources	One of the main problems facing the machine learning industry is the shortage of qualified experts with in-depth knowledge of science, technology, and mathematics. To close this gap and create a workforce equipped to handle the	(Sah & Abulaish, 2024)

	intricacies of machine learning, training, and education investments are imperative.	
Machine learning process complexity	For engineers and data scientists, the intricacy of the machine learning process, which is marked by experimental phases and ongoing modifications, presents a challenge. Errors are more likely due to ML's evolving nature and the many experiments conducted, making the process difficult and time-consuming.	(Kale et al., 2024)

4.7. Implication

Askhatuly et al. (2024) ML has a significant tool which is enhancing security defenses for attackers, it can be analyze the vast amount of data for secured the information systems. This study exploring how information systems dynamically improved and automated up- to- date the security systems using machine learning technologies. Consequently, protecting the information systems, particularly one connected to the internet, from cyber threats, attacks, damage or unauthorized access is a crucial issue that needs urgent attention (Poli, 2024). Systems security research has used a comprehensive toolkit of security best practices to reduce the likelihood of the vulnerabilities to traditional software (Aslan et al., 2023). Based on practical experience with large - scale ml systems can contribute two functional principles to guide machine learning in information security research (Bhuiyan, 2024). These principles are intended to enhance the focus and effectiveness of this research in addressing security challenges (Jaiswal & N, 2024). Threat modeling in security systems, threat modeling is crucial for understanding potential adversarial actions, predicting attack vectors, and ensuring the robustness of the systems. Threat modeling identifying and understanding potential security threats, anticipating how attackers might be exploit the systems (Rahman et al., 2024). In information security of threat modeling has no specific approach but the process often involves carefully thinking through who might want abuse the system, what capabilities they have, how they might be able to do it and what the overall risk for exploit it. machine learning driven data analytics have transformed the information security systems and financial management. In security, detection and monitoring systems now process vast amounts of data to extract actionable insights, enabling analyses that were previously unattainable (Åkerlund & Große, 2020).

5. Conclusion

The application of machine learning in the domain of information security has significantly transformed the way cyber security threats are managed. ML techniques have shown exceptional effectiveness in detecting, preventing and responding to various cyberattacks such as malware, phishing and system intrusions, which continue to evolve in complexity (Xiao, 2023). Algorithms from supervised and supervised semi supervised and reinforcement learning categories are being applied to identify malicious patterns, automate the detection process and strengthen security systems. Nevertheless, several challenges persist. These include improving data quality, ensuring real time adaptability and addressing concerns related to the transparency and clarify capacity of ML models (Ghanbari et al., 2024). Parfenov et al. (2023) adversarial attacks on ML systems End the environmental impact associated with training large scale models also present ongoing issues. Furthermore, there is a need for more comprehensive studies covering the entire ML life cycle from model development to deployment, highlighting gaps in existing research (Hossen et al., 2025). According to Shanmugam et al. (2023), Future results should focus on building more resilient ML models to counter adversarial threats, refining approaches to detect emerging threats like newly developed phishing sites and enhancing collaboration between AI experts and industry professionals (Bhuiyan et al., 2024). Advancement in deep learning privacy preserving techniques and scalable ML applications are expected to drive further progress in securing information systems.

5.1. Limitations

According to Faraji et al. (2024), Though it still has some disadvantages, machine learning has advanced significantly in recent years. Because of these drawbacks, utilizing these technologies thoughtfully is crucial because they can have major impacts on real-world applications. A true understanding is often lacking in machine learning models, which instead provide predictions based only on statistical patterns. Machine learning models lack true awareness or understanding, even though they can recognize correlations and patterns in data (König & Vellido, 2024). Artificial intelligence (AI) systems cannot generate truly original ideas, nor can they understand irony, sarcasm, or humor. As such, AI might not be able to carry out tasks requiring creativity or intuition as well as humans. Furthermore, it may be challenging to interpret machine learning algorithms applied to highly unstructured data due to intricate and difficult-to-understand relationships and patterns (Kosaraju & Buddiga, 2024). Gao et al. (2023) Furthermore, finding relevant characteristics that precisely capture the underlying patterns in such data can be difficult, making feature engineering a tedious and complex process. Preprocessing methods like data cleaning and normalization are frequently required to lessen the impact of noise and ambiguity in the data. Furthermore, machine learning algorithms might not function well in situations where the data is continuously changing or evolving (Milon et al., 2024).

5.2. Future Research

From the perspective of Abdel-Basset et al. (2024), many types of machine learning models will be applied for cloud security in the future. Nonetheless, scientists are investigating the effectiveness of different feature extraction and preprocessing methods to enhance the data quality for these algorithms. New ensemble learning strategies should be the focus of future research to improve the accuracy and robustness of machine learning models used to analyze unstructured data (Liu, 2023). The main objective of future research should be to create novel privacy-preserving methods that protect sensitive data and allow for efficient machine-learning analysis (Liu, 2023). To maximize necessary capabilities and reap the planned benefits, a comprehensive assessment of overhead should also be carried out before implementing innovations, like virtualization. Unavoidable attacks must be detected to respond thoroughly and effectively. Evaluate the dependability, accuracy, and practicality of machine learning in security-critical domains like cyber defense, monetary recognition systems, medical imaging, and diagnostics (Slathia et al., 2024). This is a major and ongoing research challenge. Examining the real-world practical uses of theoretical adversarial attacks on machine learning is another important area of research (Dayanand & Klinsega, 2024). Numerous research studies and surveys concentrate on these attacks in a theoretical setting, frequently as "white-box" attacks, which may not be as applicable in real-life scenarios. To gain a deeper understanding of these attacks' practical ramifications, it is still necessary to investigate the impact of these attacks in real-world situations and the efficacy of responses (Choi, 2024).

Acknowledgement:

Authors have appreciated to supervisor Md. Rakibul Hoque, Professor, Department of Management Information Systems, University of Dhaka for his guidelines for completing this paper.

Copyright:

References

[1] Abdel-Basset, M., Mohamed, R., & Elhoseny, M. (2024). Metaheuristic algorithms collaborated with various machine learning models for feature selection in medical data: Comparison and analysis. *Metaheuristics Algorithms for Medical Applications*, 125-145. https://doi.org/10.1016/b978-0-443-13314-5.00004-7

[2] Abdul, A., Paudel, R., & Rahman, M. M. (2023). Using machine learning algorithms to find novel biomarkers for breast cancer using RNA-SEQ dataset. https://doi.org/10.20944/preprints202309.0006.v1

[3] Abitova, G., & Abalkanov, M. (2024). Comparative analysis of ML algorithms for fraud detection. *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)*, *18*, 554-559. https://doi.org/10.1109/sist61555.2024.10629283

[4] Poli, T. A. (2024). Mediating Role of Entrepreneurship Capability in Sustainable Performance and Women Entrepreneurship: An Evidence from a Developing Country. *Journal of Ecohumanism, 3*(3), 2006-2019.

[5] Abu Dabous, S., Alzghoul, A., & Ibrahim, F. (2024). Intelligent condition prediction model for bridge infrastructure based on evaluating machine learning algorithms. *Smart and Sustainable Built Environment.* https://doi.org/10.1108/sasbe-02-2024-0059

[6] Åkerlund, A., & Große, C. (2020). Integration of data envelopment analysis in business process models: A novel approach to measure information security. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 281-288. https://doi.org/10.5220/0008875802810288,

[7] Amin, A., Bhuiyan, M. R. I., Hossain, R., Molla, C., Poli, T. A., & Milon, M. N. U. (2024). The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country. *Business Strategy & Development*, 7(2), e363. https://doi.org/10.1002/bsd2.363

[8] Ammannamma, T., & Vandana, D. (2023). undefined. *International Journal for Research in Applied Science and Engineering Technology, 11*(6), 4948-4953. https://doi.org/10.22214/ijraset.2023.54218

[9] Milon, M. N. U. (2024). Gravitating towards Artificial Intelligence on Anti-Money Laundering A PRISMA Based Systematic Review. *International Journal of Religion, 5*(7), 303-315.

[10] Anzum, F., Asha, A. Z., Dey, L., Gavrilov, A., Iffath, F., Ohi, A. Q., Pond, L., Shopon, M., & Gavrilova, M. L. (2024). A comprehensive review of trustworthy, ethical, and explainable computer vision advancements in online social media. *Advances in Information Security, Privacy, and Ethics*, 1-46. https://doi.org/10.4018/978-1-6684-8127-1.ch001

[11] Askhatuly, A., Berdysheva, D., Yedilkhan, D., & Berdyshev, A. (2024). Security risks of ML models: Adverserial machine learning. *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)*, 440-446. https://doi.org/10.1109/sist61555.2024.10629452

[12] 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. https://doi.org/10.3390/electronics12061333

[13] Azoff, E. M. (2024). AI and machine learning. *Toward Human-Level Artificial Intelligence*, 2-4. https://doi.org/10.1201/9781003507864-2

[14] Bertino, E., Bhardwaj, S., Cicala, F., Gong, S., Karim, I., Katsis, C., Lee, H., Li, A. S., & Mahgoub, A. Y. (2023). Challenges in the use of ML for security. *Synthesis Lectures on Information Security, Privacy, and Trust*, 131-143. https://doi.org/10.1007/978-3-031-28259-1_9

[15] Bhuiyan, M. R. I. (2023). The Challenges and Opportunities of Post-COVID Situation for Small and Medium Enterprises (SMEs) in Bangladesh. *PMIS Review, 2*(1), 141-159. http://dx.doi.org/10.56567/pmis.v2i1.14

[16] Bhuiyan, M. R. I. (2024). Examining the digital transformation and digital entrepreneurship: A PRISMA based systematic review. Pakistan Journal of Life and Social Sciences, 22(1), 1136-1150. http://dx.doi.org/10.57239/PJLSS-2024-22.1.0077

[17] Bhuiyan, M. R. I., Akter, M. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. *Journal of Science and Technology Policy Management.* Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSTPM-10-2023-0170

[18] Bhuiyan, M. R. I., Faraji, M. R., Rashid, M., Bhuyan, M. K., Hossain, R., & Ghose, P. (2024). Digital Transformation in SMEs Emerging Technological Tools and Technologies for Enhancing the SME's Strategies and Outcomes. *Journal of Ecohumanism, 3*(4), 211-224. https://doi.org/10.62754/joe.v3i4.3594

[19] Bhuiyan, M. R. I., Hossain, R., Rashid, M., Islam, M. M., Mani, L., & Milon, M. N. U. (2024). Gravitating the components, technologies, challenges, and government transforming strategies for a Smart Bangladesh: A PRISMA-based review. *Journal of Governance and Regulation, 13*(3), 177–188. https://doi.org/10.22495/jgrv13i3art15

[20] Bhuiyan, M. R. I., Milon, M. N. U., Hossain, R., Poli, T. A., & Salam, M. A. (2024). Examining the Relationship between Poverty and Juvenile Delinquency Trends in a Developing Country. *Academic Journal of Interdisciplinary Studies*, 13(6), 255-274.

[21] Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy: An Empirical Study in Bangladesh. doi: 10.20944/preprints202307.1652.v1

[22] Bhuiyan, M. R. I., Ullah, M. W., Ahmed, S., Bhuyan, M. K., & Sultana, T. (2024). Information Security for An Information Society for Accessing Secured Information: A PRISMA Based Systematic Review. *International Journal of Religion, 5*(11), 932-946. https://doi.org/10.61707/frfnr583

[23] Bhuiyan, M. R., & Akter, M. (2024). Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review. *Journal of Information Systems and Informatics, 6*(1), 245-269. https://doi.org/10.51519/journalisi.v6i1.659

[24] Boulsane, H. A., & Afdel, K. (2024). undefined. https://doi.org/10.2139/ssrn.4897866

[25] Chi, J., Guo, S., Zhang, H., & Shan, Y. (2023). L-ghostnet: Extract better quality features. *IEEE Access, 11*, 2361-2374. https://doi.org/10.1109/access.2023.3234108

[26] Choi, S. (2024). Transnational terrorist attacks. *Oxford Research Encyclopedia of International Studies.* https://doi.org/10.1093/acrefore/9780190846626.013.859

[27] Daphin Lilda, S., & Jayaparvathy, R. (2023). Machine learning techniques in ECG data analysis for medical applications. *Handbook of AI-Based Models in Healthcare and Medicine*, 226-246. https://doi.org/10.1201/9781003363361-13

[28] Dasari, N., & Samanta, I. (2024). Intelligent authentication gateway: Bridging the gap between traditional and FIDO2 security through AI/ML enhancement. https://doi.org/10.31224/3699

[29] Dayanand, Wilson Jeberson, & Klinsega Jeberson. (2024). Machine learning defenses: Exploring the integration of machine learning techniques within CAPTCHA systems to dynamically adjust challenge difficulty and thwart

adversarial attacks. *International Journal of Scholarly Research in Multidisciplinary Studies*, *4*(2), 001-007. https://doi.org/10.56781/ijsrms.2024.4.2.0030

[30] Dhibar, K., & Maji, P. (2023). Future outlier detection algorithm for smarter industry application using ML and AI. *Advances in Systems Analysis, Software Engineering, and High Performance Computing*, 152-166. https://doi.org/10.4018/978-1-6684-8785-3.ch008

[31] Divya, R., Gaganashree, Devamane, S. B., Dharshini, V., & Deepika, S. (2023). Performance analysis of machine learning algorithms for password strength check. *2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA)*,

[32] Faraji, M. R., Shikder, F., Hasan, Md. H., Islam, Md. M., & Akter, U. K. (2024). Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions. *International Journal of Religion*, *5*(10), 4766–4782. https://doi.org/10.61707/7rfyma13

[33] Fung, C., Zeng, E., & Bauer, L. (2024). Attributions for ML-based ICS anomaly detection: From theory to practice. *Proceedings 2024 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2024.23216

[34] Gao, W., Zhang, L., & Cao, Q. (2023). Curriculum reform of sampling techniques based on machine learning algorithms: A panel data analysis. *2023 International Conference on Algorithms, Computing and Data Processing (ACDP)*, *35*, 50-55. https://doi.org/10.1109/acdp59959.2023.00016

[35] Garai, M. S., Paul, R. K., & Yeasin, M. (2023). Ceemdanml: Ceemdan decomposition based hybrid machine learning models. *CRAN: Contributed Packages*. https://doi.org/10.32614/cran.package.ceemdanml

[36] Ghanbari, A., Shirdel, G. H., & Maleki, F. (2024). Semi-self-Supervised domain adaptation: Developing deep learning models with limited annotated data for wheat head segmentation. *Algorithms*, *17*(6), 267. https://doi.org/10.3390/a17060267

[37] Gonaygunta, H. (2023). Machine learning algorithms for detection of cyber threats using logistic regression. *International Journal of Smart Sensor and Adhoc Network*, 36-42. https://doi.org/10.47893/ijssan.2023.1229

[38] Gupta, A., Singh, B., & Chaudhary, N. (2023). Assessing intrusion detection process using ML techniques: Issues, options, and potential future directions. *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, *44*, 1-6.

[39] Haddaway, N. (2022). Citationchaser: Perform forward and backwards chasing in evidence syntheses. *CRAN: Contributed Packages*. https://doi.org/10.32614/cran.package.citationchaser

[40] Hocking, T. (2023). Mlr3resampling: Resampling algorithms for 'mlr3' framework. *CRAN: Contributed Packages*. https://doi.org/10.32614/cran.package.mlr3resampling

[41] Hooda, A. (2024). Adaptive real-time big data processing framework: A machine learning and reinforcement learning approach using random forest and Q-learning for dynamic resource management. https://doi.org/10.21203/rs.3.rs-4962286/v1

[42] Hossain, R., Al- Amin, A.-A., Mani, L., Islam, M. M., Poli, T. A., & Milon, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country. *WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS*, *21*,1392–1408. https://doi.org/10.37394/23207.2024.21.114

[43] Hossain, R., Ghose, P., Chowdhury, T. M., Hossen, M. D., Hasan, M. N., & Mani, L. (2024). Ownership Structures and Firm Performance: A Correlation and Regression Analysis of Financial Institutions in Bangladesh. Pak. j. life soc. Sci. 22(2): 6278-6295. https://doi.org/10.57239/PJLSS-2024-22.2.00473

[44] Hossen, M. D., Abedin, M. Z., Chowdhury, T. M., Islam, Z., & Kabir, M. R. (2025). Unveiling the Impact of E-Governance on the Transformation from Digital to Smart Bangladesh. Pakistan Journal of Life & Social Sciences, 23(1). https://doi.org/10.57239/PJLSS-2025-23.1.009

[45] Islam, M. A., & Bhuiyan, M. R. I. (2022). Digital Transformation and Society. Available at SSRN: https://ssrn.com/abstract=4604376 or http://dx.doi.org/10.2139/ssrn.4604376

[46] Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., & Mani, L. (2024). Gravitating towards Internet of Things: Prospective Applications, Challenges, and Solutions of Using IoT. *International Journal of Religion*, *5*(2), 436-451. https://doi.org/10.61707/awg31130

[47] Jain, A. (2022). Real-time and context-based approach to provide users with recommendations for scaling of cloud resources using machine learning and recommendation systems. *Lecture Notes on Data Engineering and Communications Technologies*, 355-362. https://doi.org/10.1007/978-981-19-2347-0_27

[48] Jaiswal, R., & N, G. (2024). undefined. *International Journal of Research Publication and Reviews*, *5*(3), 928-931. https://doi.org/10.55248/gengpi.5.0324.0635

[49] Jo, T. (2020). Simple machine learning algorithms. *Machine Learning Foundations*, 69-90. https://doi.org/10.1007/978-3-030-65900-4_4

[50] Joshi, S., & Oza, N. (2024). Enhanced network security against SQL injection attack using machine learning. https://doi.org/10.21203/rs.3.rs-4362691/v1

[51] Kaigorodtsev, A. A., & Kaigorodtseva, T. F. (2020). Problems of ensuring information security in Russia in the conditions of digitalization. *Society and Security Insights*, *3*(3), 79-89. https://doi.org/10.14258/ssi(2020)3-06

[52] Kale, K. D., More, P., & Singh, P. (2024). Exploratory data analysis of the Monkeypox virus using machine learning. *The 3rd International Electronic Conference on Processes&mdash;Green and Sustainable Process Engineering and Process Systems Engineering*, 118. https://doi.org/10.3390/proceedings2024105118

[53] Kilpatrick, S. E. (2024). Atypical lipomatous tumor/well differentiated liposarcoma and related mimics with updates. When is molecular testing most cost-effective, necessary, and indicated? *Human Pathology*, *147*, 82-91.

https://doi.org/10.1016/j.humpath.2023.12.005

[54] König, C., & Vellido, A. (2024). undefined. https://doi.org/10.21203/rs.3.rs-4478926/v1

[55] Kosaraju, D., & Buddiga, P. (2024). Shaping the future of AI: How human guidance can cultivate responsible LLMs. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(2), 445-449. https://doi.org/10.51219/jaimld/pranitha-buddiga/123

[56] Kumari, I., Chatterjee, I., & Lee, M. (2023). Development of ML-based methodologies for adaptive intelligent E-learning systems and time series analysis techniques. *Machine Learning Applications*, 11-30. https://doi.org/10.1002/9781394173358.ch2

[57] Liu, H. (2023). undefined. *Proceedings of the 1st International Conference on Data Analysis and Machine Learning*, 494-499. https://doi.org/10.5220/0012800600003885

[58] Liu, H., Qu, W., Jia, J., & Gong, N. Z. (2024). Pre-trained encoders in self-supervised learning improve s Park, H., & Kim, S. (2023). Software overview for on-device AI and ML benchmark in smartphones. *Artificial Intelligence and Hardware Accelerators*, 151-165.https://doi.org/10.1007/978-3-031-22170-5_5

[59] Liu, M. (2023). Solving real-world problems with machine learning. *Machine Learning, Animated*, 301-320. https://doi.org/10.1201/b23383-16

[60] Lyubchyk, L., & Yamkovyi, K. (2022). Comparative analysis of modified semi-supervised learning algorithms on a small amount of labeled data. *System research and information technologies*, (4), 34–43. https://doi.org/10.20535/srit.2308-8893.2022.4.03

[61] Mani, L. (2024). Gravitating towards the Digital Economy: Opportunities and challenges for transforming smart Bangladesh. *Pakistan Journal of Life and Social Sciences*, *22*(1), 3324-3334. https://doi.org/10.57239/PJLSS-2024-22.1.00241

[62] Meng, J. (2024). AI as an employee: How AI affects managers evaluation of creative works. *AEA Randomized Controlled Trials*. https://doi.org/10.1257/rct.14071-1.0

[63] Mihalache, R., Gavriluţ, D., & Anton, D. (2024). Real-time deep learning-based malware detection using static and dynamic features. *Proceedings of the 16th International Conference on Agents and Artificial Intelligence*, 226-234. https://doi.org/10.5220/0012316800003636

[64] Mihalache, R., Gavriluţ, D., & Anton, D. (2024). Real-time deep learning-based malware detection using static and dynamic features. *Proceedings of the 16th International Conference on Agents and Artificial Intelligence*, 226-234. https://doi.org/10.5220/0012316800003636

[65] Milon, M. N. U., Ghose, P., Pinky, T. C., Tabassum, M. N., Hasan, M. N., & Khatun, M. (2024). An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era. Edelweiss Applied Science and Technology, 8(4), 2072-2093. https://doi.org/10.55214/25768484.v8i4.1583

[66] Mire, A. V., Elangovan, V., & Dhote, B. (2021). Comprehensive analysis of dimensionality reduction techniques for machine learning applications. *Design of Intelligent Applications Using Machine Learning and Deep Learning Techniques*, 61-76. https://doi.org/10.1201/9781003133681-4

[67] Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic Review. *Migration Letters*, *20*(S9), 927-945. https://doi.org/10.59670/ml.v20iS9.4918

[68] Nanath, K., & Rahman, A. (2022). Cracking Captcha using machine learning algorithms: An intersection of Captcha categories and ML algorithms. *Machine Learning for Cyber Security*, 27-40. https://doi.org/10.1515/9783110766745-002

[69] Niknami, N., & Wu, J. (2024). Advanced ML/DL-based intrusion detection systems for software-defined networks. *Advances in Information Security*, 121-146. https://doi.org/10.1007/978-3-031-53510-9_5

[70] Özaşçılar, M., Çalıcı, C., & Vakhitova, Z. (2024). Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety*, *26*(1), 112-128. https://doi.org/10.1057/s41300-024-00201-y

[71] Padole, G., Annareddy, R. R., Mothukuri, A., Aela, A., & Varma, K. (2024). undefined. https://doi.org/10.21203/rs.3.rs-4324837/v1

[72] Parhizkari, S. (2024). Anomaly detection in intrusion detection systems. *Artificial Intelligence*. https://doi.org/10.5772/intechopen.112733

[73] Pasrija, P., Singh, U., & Khurana, M. (2024). Performance analysis of intrusion detection system using ML techniques. *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*, 135-150. https://doi.org/10.1002/9781394196470.ch8

[74] Paya, A., Arroni, S., García-Díaz, V., & Gómez, A. (2024). Apollon: A robust defense system against adversarial machine learning attacks in intrusion detection systems. *Computers & Security*, *136*, 103546. https://doi.org/10.1016/j.cose.2023.103546

[75] Pearson, W. S. (2024). Research topics in applied linguistics as keywords from authors and keywords from abstracts: A bibliometric study. *A Scientometrics Research Perspective in Applied Linguistics*, 113-134. https://doi.org/10.1007/978-3-031-51726-6_5

[76] Pinsky, E., & Piranavakumar, K. (2024). A machine learning-based approach to analyze and visualize time-series sentencing data. *ITISE 2024*, *33*, 50. https://doi.org/10.3390/engproc2024068050

[77] Qin, X., Yao, P., Liu, M., Cheng, X., Shi, F., & Guo, L. (2024). Robust classification of incomplete time series with noisy labels. *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2620-2625.

https://doi.org/10.1109/cscwd61410.2024.10580639

[78] Rahman, Md. M., Islam, Md. M., Khatun, M., Uddin, S., Faraji, M. R., & Hasan, Md. H. (2024). Gravitating towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *22*(1). https://doi.org/10.57239/PJLSS-2024-22.1.0089

[79] Rai, R., Rohilla, A., & Rai, A. (2024). Impact of artificial intelligence (AI) and machine learning (ML) on cloud security. *Advances in Information Security, Privacy, and Ethics*, 111-124. https://doi.org/10.4018/979-8-3693-3249-8.ch006

[80] Raj, P., & Saundharya Thejaswini, R. (2022). Machine learning (ML) on the Internet of things (IoT) streaming data toward real-time insights. *Streaming Analytics: Concepts, architectures, platforms, use cases and applications*, 405-432. https://doi.org/10.1049/pbpc044e_ch18

[81] Reed, J., & Macalla, C. (2022). How much better could we have done? Using a time machine method to quantify the impact of incremental geologic data on machine learning forecast accuracy. *Proceedings of the 10th Unconventional Resources Technology Conference.*

[82] Ringel, S. (2023). An ethnography for studying HMC: What can we learn from observing how humans communicate with machines? *The Sage Handbook of Human–Machine Communication*, 236-242. https://doi.org/10.4135/9781529782783.n29

[83] Robledo, S., Zuluaga, M., Arbelaez Echeverry, O., & Valencia Hernandez, L. A. (2021). Tosr: Create the tree of science from wos and Scopus. *CRAN: Contributed Packages.* https://doi.org/10.32614/cran.package.tosr

[84] Rose, J., Swann, M., Bendiab, G., & Shiaeles, S. (2022). 5. cyber-threat detection in the IoT. *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation.* https://doi.org/10.1561/9781680838350.ch5

[85] Sabarmathi, G., & Chinnaiyan, R. (2021). Machine learning approaches in big data analytics optimization for wireless sensor networks. *Machine Learning and Deep Learning Techniques in Wireless and Mobile Networking Systems*, 79-95. https://doi.org/10.1201/9781003107477-5

[86] Sah, A. K., & Abulaish, M. (2024). DeepCKID: A multi-head attention-based deep neural network model leveraging Classwise knowledge to handle Imbalanced textual data. *Machine Learning with Applications*, *17*, 100575. https://doi.org/10.1016/j.mlwa.2024.100575

[87] Shanmugam, L., Tillu, R., & Jangoan, S. (2023). Privacy-preserving AI/ML application architectures: Techniques, trade-offs, and case studies. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 398-420. https://doi.org/10.60087/jklst.vol2.n2.p420

[88] Singhal, S. (2024). Data privacy, compliance, and security including AI ML. *Advances in Systems Analysis, Software Engineering, and High Performance Computing*, 111-126. https://doi.org/10.4018/979-8-3693-2909-2.ch009

[89] Slathia, H., Bakshi, V., & Sharma, P. (2024). Machine learning innovations in polycystic ovarian syndrome diagnosis: A comprehensive review. *Lecture Notes in Networks and Systems*, 603-617. https://doi.org/10.1007/978-981-97-2550-2_43

[90] Son, N. T., Van Bien, N., Quynh, N. H., & Tho, C. C. (2022). Machine learning based admission data processing for early forecasting students' learning outcomes. *International Journal of Data Warehousing and Mining*, *18*(1), 1-15. https://doi.org/10.4018/ijdwm.313585

[91] Sundaram Nanhay Singh, S. (2023). Financial fraud detection of digital transaction using artificial intelligence & Machine learning. *International Journal of Science and Research (IJSR)*, *12*(4), 125-129. https://doi.org/10.21275/sr23329162725

[92] UDDIN, K. S., BHUIYAN, M. R. I., & HAMID, M. (2024). Perception towards the Acceptance of Digital Health Services among the People of Bangladesh. *WSEAS Transactions on Business and Economics*, 21:1557-1570 https://doi.org/10.37394/23207.2024.21.127

[93] Varma, A., Kumar, A. T., & B, Y. (2024). Detection and prevention of distributed denial of service (DDoS) attacks using machine learning techniques. *2024 2nd International Conference on Networking and Communications (ICNWC)*, 1-5. https://doi.org/10.1109/icnwc60771.2024.10537405

[94] Wang, T., Reiffsteck, P., Chevalier, C., Chen, C., & Schmidt, F. (2023). Machine learning (ML) based predictive maintenance policy for bridges crossing waterways. *Transportation Research Procedia*, *72*, 1037-1044. https://doi.org/10.1016/j.trpro.2023.11.533

[95] Watanabe, R., Matsunaka, T., Kubota, A., & Urakawa, J. (2023). Machine learning based prediction of vulnerability information subject to a security alert. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 313-320.

[96] Xiao, P. (2023). Malware cyber threat intelligence system for Internet of things (IoT) using machine learning. *Journal of Cyber Security and Mobility.* https://doi.org/10.13052/jcsm2245-1439.1313

[97] Yang, S., Lee, J., Sezgin, E., Bridge, J., & Lin, S. (2021). Clinical advice by voice assistants on postpartum depression: Cross-sectional investigation using Apple Siri, Amazon Alexa, Google assistant, and Microsoft Cortana. *JMIR mHealth and uHealth*, *9*(1), e24045. https://doi.org/10.2196/24045

[98] Yeldho, N., Thomas, D., Kurian, V. G., Arathy, C., & Biju, A. V. (2024). Are machine learning models effective in predicting emerging markets? Investigating the accuracy of predictions in emerging stock market indices. *Quality & Quantity.* https://doi.org/10.1007/s11135-024-01964-0