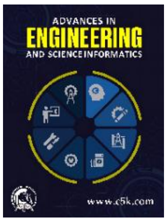
Advances in Engineering and Science Informatics

"Volume 1, Issue 1, Year 2024"
website: https://www.c5k.com



Research Article

Machine Learning Models for Cybersecurity in the USA firms and develop models to enhance threat detection

Md Shawon Islam

Department of Electrical & Electronic Engineering, Mymensingh Engineering College (University of Dhaka), Mymensingh-2208, Bangladesh

**Corresponding Author:* shawonislam9955@gmail.com

ARTICLE INFO

Article history:
06 Jul 2024 (Received)
18 Aug 2024 (Accepted)
26 Aug 2024 (Published Online)

Keywords:
Cybersecurity, Cyberattack, Machine Learning, Cumulative Abnormal Returns (CAR), Threats

ABSTRACT

In the context of global digitalization trends, the problem of the impact of cyberattacks on the company is significantly relevant. The rapid evolution and growth of the internet through the last decades led to more concern about cyber-attacks that are continuously increasing and changing. As a result, an effective intrusion detection system was required to protect data, and the discovery of machine learning is one of the most successful ways to address this problem. This article is devoted to the impact of cyberattacks on the US firms' market value since it is an indicator of firm performance and how it can be solved by using machine learning technology. The paper's central hypothesis is the assumption that a cyberattack announcement is supposed to change market reaction, which is predicted to be harmful since cybercrime incidents can lead to high implicit and explicit costs. The paper explores the effect of firm-specific and attack-specific characteristics of cyberattacks on the CAR (Cumulative Abnormal Returns) with the data of cyberattacks for US firms from 2011 to 2020. The previously used security systems are no longer sufficient because cybercriminals are smart enough to evade conventional security systems. Conventional security systems lack efficiency in detecting previously unseen and polymorphic security attacks. Machine learning (ML) techniques are playing a vital role in numerous applications of cyber security. It discusses recent machine learning work with various network implementations, applications, algorithms, learning approaches, and datasets to develop an operational intrusion detection system in cybersecurity. This work should serve as a guide for new researchers and those who want to immerse themselves in the field of machine learning techniques within cybersecurity in US firms.

DOI: https://doi.org/10.103/xxx @ 2024 Advances in Engineering and Science Informatics (AESI), C5K Research Publication

1. Introduction

Population uses the Internet and this figure increases up to 78% in the developed countries (Union, 2014). The North Atlantic Treaty Organization (NATO) identifies the internet as "a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development" (Hathaway & Klimburg, 2012). Numerous descriptions are made about cyber security in the literature. According to Canongia and Mandarino, "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure" (Canongia & Mandarino, 2012). Cyber security is a significant research area because all of the operations based on government, military, commercial, financial and civilians gather, process, and store tremendous volume of data on computers and others (Dua & Du, 2016; Twomey, 2010). Cyber security is to protect the integrity of the data, networks, and programs from cyber threats to cyberspace (Dan et al., 2014).

The introduction machine learning algorithms into cybersecurity frameworks represents a paradigm shift in defense strategies, moving away from traditional rule-based approaches towards more adaptive and proactive methodologies. This shift is propelled by the realization that conventional cybersecurity measures, reliant primarily on signature-based detection systems and static rule sets, are increasingly inadequate in addressing the dynamic and sophisticated nature of modern cyber threats. Currently, machine learning and deep learning models are being applied almost in all areas of cyber security to detect and respond against cyberattacks (Prasad et al., 2020).

*Corresponding author: shawonislam9955@gmail.com (Md Shawon Islam)
All rights are reserved @ 2024 https://www.c5k.com, https://doi.org/10.103/xxx
Cite: Md Shawon Islam (2024). Machine Learning Models for Cybersecurity in the USA firms and develop models to enhance threat detec tion. *Advances in Engineering and Science Informatics,* 1(1), pp. 17-26.

Consequently, the integration of machine learning techniques holds immense promise in fortifying cyber defenses, offering the agility, scalability, and predictive capabilities necessary to thwart cyberattacks effectively. At the heart of ML-driven cybersecurity lies the ability to harness the power of data. Machine learning algorithms, fueled by vast amounts of labeled and unlabeled data, possess the capability to discern intricate patterns and anomalies indicative of malicious activities within complex and diverse datasets. By analyzing historical attack data, user behavior, network traffic, and system logs, these algorithms can identify subtle indicators of compromise, enabling early detection and mitigation of cyber threats before they inflict substantial damage.

Moreover, the adaptive nature of machine learning algorithms empowers cybersecurity systems to evolve in tandem with the rapidly changing threat landscape. Through continuous learning and refinement, these algorithms enhance their efficacy in detecting novel and previously unseen threats, thereby augmenting the resilience of cyber defense mechanisms. This adaptability is particularly critical in combating sophisticated cyber adversaries who employ stealthy, polymorphic, and zero-day attack techniques to evade detection. Despite the considerable promise of ML in bolstering cybersecurity defenses, the integration of these technologies presents novel challenges and ethical dilemmas. Concerns surrounding data privacy, algorithmic bias, and unintended consequences necessitate careful consideration and mitigation strategies to ensure the responsible and ethical deployment of ML-driven cybersecurity solutions. Moreover, the rapid pace of technological innovation and the dynamic nature of cyber threats mandate continuous monitoring, adaptation, and collaboration across stakeholders to stay ahead of emerging risks and vulnerabilities.

In light of these considerations, this paper seeks to provide a comprehensive overview of ML-driven cybersecurity, examining the underlying principles, applications, challenges, and future directions. By synthesizing insights from academia, industry, and government sectors, this research aims to contribute to the ongoing discourse on the role of ML in shaping the future of cybersecurity and fostering a more secure and resilient digital ecosystem. In recent years, many are the organizations and projects have been created with the aim of facing these threats. One of them is the Open Web Application Security Project (OWASP), an international non-for-profit charitable organization that focuses on the application security (Khorshidpour et al., 2018). They identify a series of software vulnerabilities and describe the ten most important in their top ten project, whose latest report was published in 2013 and included the following security risks (Ananda Kumar et al., 2014): injection, broken authentication and session management, cross-site scripting (XSS), insecure direct object references, security misconfiguration, sensitive data exposure, missing function level access control, cross-site request forgery (CSRF), using components with known vulnerabilities, and unvalidated redirects and forwards. With similar philosophy, Microsoft's Security Development Lifecycle offers developers information and tools to build secure software ((NATO, 2008). Through interdisciplinary collaboration and knowledge-sharing, we can harness the transformative potential of ML to address the evolving cyber threat landscape and safeguard the integrity, confidentiality, and availability of critical information assets. However the aim of this paper is the study of cybersecurity in US firms, applying machine learning to detect threats on cybersecurity and briefly discuss on the solution of different problem on cybersecurity through algorithms.

2. Literature Review

Research on the connection between cybersecurity breaches and a company's market value is now abundant. There is a suggestion that the cumulative abnormal returns (CAR) of publicly traded corporations are adversely affected when cybersecurity problems are announced. Cybersecurity breaches involving lost private information have been found to have a considerable negative influence on CAR (Campbell et al., 2003). A 2009 investigation by Goel and Shawky found that cyberattacks reduced the market value. After looking at the effects of cybersecurity breaches, Cavusoglu et al. (2004) found that the market value of the company decreased by 2.1%. Furthermore, they have determined that the negative effect varies according to the kind of occurrence, the type of firm, and its size. The literature on ML-driven cybersecurity underscores the transformative potential of machine learning algorithms in enhancing defense mechanisms against evolving cyber threats. In their study, Smith et al. (2020) conducted a comprehensive analysis of machine learning techniques for malware detection, emphasizing the efficacy of supervised learning models in accurately classifying malicious software based on behavioral patterns and code analysis. As indicated in Fig. 1 there are three main techniques to machine learning: supervised, unsupervised, semi-supervised, and reinforcement learning. Supervised learning is based on labeled data, unsupervised learning is based on unlabelled data, and semi-supervised learning is based on both.

Their findings revealed that ensemble methods, such as Random Forest and Gradient Boosting, outperformed traditional signature-based approaches, achieving higher detection rates and lower false positive rates across diverse malware families. Moreover, research by Johnson and Chen (2019) focused on the application of deep learning algorithms, particularly convolutional neural networks (CNNs), in detecting network intrusions and anomalous activities. By leveraging the temporal and spatial dependencies inherent in network traffic data, CNN-based intrusion detection systems demonstrated superior performance in identifying stealthy and previously unseen attacks, including zero-day exploits and polymorphic malware variants. The study highlighted the importance of feature extraction and representation learning in capturing intricate enhancing the overall accuracy and robustness of intrusion detection systems.

In addition to malware detection and network security, ML-driven techniques have been increasingly utilized in the realm of threat intelligence and predictive analytics. Research by Liang et al. (2021) examined the role of machine learning algorithms in forecasting cyberattacks and identifying emerging threats through anomaly detection and trend analysis. By analyzing historical attack data and contextual information, predictive models equipped with recurrent neural networks

(RNNs) and long short-term memory (LSTM) architectures demonstrated the ability to anticipate future attack vectors and prioritize defensive actions proactively. The study highlighted the significance of real-time threat intelligence in preemptively mitigating cyber risks and minimizing the impact of security patterns indicative of malicious behaviors, thereby incidents on organizational assets. Neethu B. represents a framework that is PCA for feature selection with Naive Bayes to develop a network intrusion detection system. In this study, the KDD Cup 1999 intrusion detection benchmark dataset is preferred for experiments. The results show that the performance of this method achieves a higher detection rate, is less time-consuming, and has a low cost factor compared to the neural network and tree algorithm-based approach. In addition, the proposed system provides about 94% accuracy (Neethu, 2013). Fig.1. shows the technique of machine learning

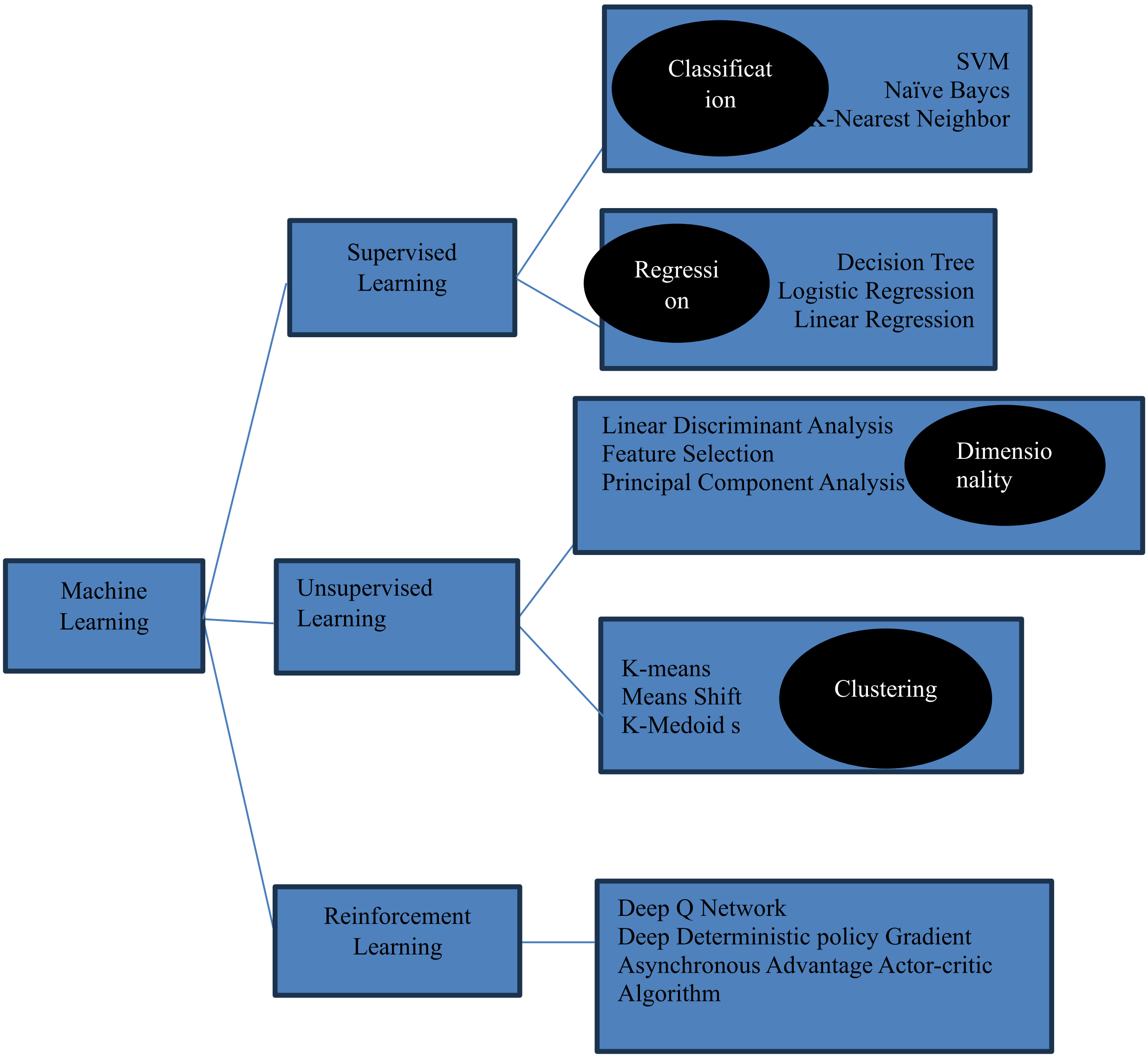


Fig. 1. Some techniques of Machine learning.

Rafal et al. presented a novel method for detecting cyberattacks targeting web applications. This method was compared with Naive Bayes, AdaBoost, Part and J48, which are machine learning algorithms. In addition, the CSIC 2010 HTTP Dataset is used for the assessment of the proposed model. This study specifically focused on solutions that use HTTP protocols to communicate clients with the servers. The authors claimed that this model is able to obtain a higher detection percentage while having a lower false positive rate. At the same time, the results show that the J48 method is the best approach for this problem and the true-positive value is around 0.04 (Kozik et al., 2014).

Zamani and Movahedi represent several models for detecting intrusion. In this study, these models are divided based on classical machine learning (ML) and based on computational intelligence (CI) such as genetic algorithms and fuzzy logic. They conducted various experiments and compared their algorithms' performance. Experimental results show that the decision tree algorithm has achieved the best results.

On the other hand, this study explained how different features of CI models could be used to build effective IDS (Zamani & Movahedi, 2013). Other recent ML-based approaches to insider threat detection include supervised learning (Gavai et al., 2015) and stream online learning (Tuor et al., 2017). Gavai et al. applied different ML methods to organizational data to detect not only anomalies but also early "quitter" indicators, where both may suggest insider threats (Gavai et al., 2015). Capabilities of different ML techniques, such as decision trees (Le & Zincir-Heywood, 2019), Bayesian-based approaches (Roberts et al., 2016), and self-organizing maps (Le & Zincir-Heywood, 2018) were also examined for insider threat detection. Stream online learning approaches were employed in an attempt to characterize conditions of non-stationary user behaviors. With this in mind, the moving weighted average is a common technique to support anomaly detection under streaming conditions (Parveen & Thuraisingham, 2012). In (Tuor et al., 2017), Tuor et al. proposed an anomaly detection approach using a deep neural network (one model for the organization), or recurrent neural networks (one model per user), to produce anomaly scores. Bose et al. proposed a system employing scalable supervised and unsupervised learning algorithms on a fusion of heterogeneous data streams to detect anomalies and insider threats (Böse et al., 2017).

In this paper, as distinct from previous work in the literature, this paper presents a user-centered insider threat detection system in cybersecurity in US firms, where data analytics is employed on multiple levels of data granularity under different training conditions. To the best of our knowledge, this is the first work comprehensively assessing the effect of cybersecurity in US firms and Developing models to enhance threat detection in cybersecurity in US firms using machine learning techniques.

3. Methodology

The event study methodology is used in this research to investigate the impact of announcements about cybersecurity breaches on a firm's market performance. The event study helps to examine cumulative abnormal returns caused by security breach incidents. According to Stanford computer science professor Andrew Ng, Machine learning (ML) is "the science of getting computers to act without being explicitly programmed (Torrano-Gimenez et al., 2011)". The workflow is designed to be modular and easily expandable for a wide range of corporate environments, data acquisition conditions, as well as learning and analysis methods. The Cybersecurity Disclosure Day is taken as an "event" to study the impact of breaches on the market value of US firms. A new dataset of US firms for the 2011-2020 period is used to verify previous studies that have found a negative impact of cyberattacks on shareholders' wealth. The number of cybersecurity incidents for the USA companies is collected from the Audit Analytics database. The initial sample of the cybersecurity breaches contains 674 observations. Two observations without indicated event date and six observations without information about firm characteristics such as sic code are deleted. The sample consists of 666 observations for that period. Table 1 shows the annual frequency of cybersecurity breaches from 2011-2020 [30].

Table 1. The number of cybersecurity breaches per year.

Year	**Number of incidents**	**Percentage**
2011	24	3.59
2012	29	4.35
2013	39	5.86
2014	55	8.26
2015	41	6.16
2016	49	7.36
2017	82	12.31
2018	102	16.37
2019	133	19.97
2020	105	15.77
Total	**666**	**100**

The chronological distributions of 666 cyberattacks over the period 2011 to 2020 by industry are presented in Table 2.

Table 2. Distribution of Cyberattacks by Industry [31]

Industry type	**Number of incidents**	**Percentage**
Mining, gas, and oil field	2	0.3
Construction	2	0.3
Manufacturing	160	24.03
Transport, communications	93	13.96
Wholesale trade	17	2.55
Retail trade	95	14.26
Finance	102	15.32
Service industries	195	29.28
Total	**666**	**100**

AI is a field of scientific research to increase computing power, to develop productive algorithms and well-organized knowledge. AI applies to solving complicated problems that cannot be solved without combining intelligence, discovering the hidden patterns in data and developing intelligent machines (Torrano-Gimenez et al., 2011). Artificial Neural Networks (ANNs), which is a technique of AI, are a set of computer algorithms that are biologically inspired to simulate how the human brain neuron processes information (Torrano-Gimenez et al., 2011). ANNs gather their knowledge by detecting the patterns and relationships among data and learn through their architectures, transfer functions and learning algorithms (Torrano-Gimenez et al., 2011). There are many types of neural networks for various applications available in the literature (Torrano-Gimenez et al., 2011). Multilayered perceptron (MLP) type neural networks are the simplest and most commonly used neural network architectures (Torrano-Gimenez et al., 2011). MLPs are trained with many learning algorithms. Levenberg-Marquardt (LM) is one of the most preferred training algorithms for MLPs.

The principal interest of this research is to assess the capability of ML techniques in detecting insider threats in firms. For the process Fig. 2 is given below.

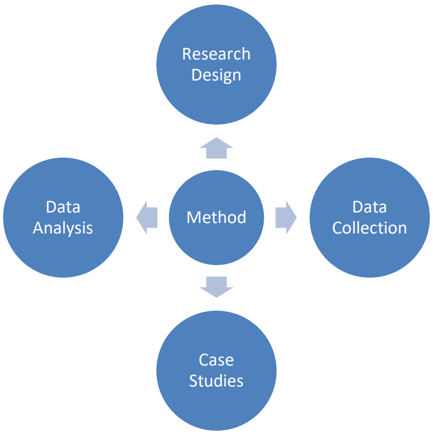


Fig. 2. Research Method.

Research Design: Adopt a mixed-methods approach, integrating quantitative and qualitative analyses to explore the multifaceted dimensions of ML-driven cybersecurity comprehensively. Utilize a combination of literature review, empirical studies, and case analyses to capture diverse perspectives and insights within the field.

Data Collection: Gather data from scholarly articles, research papers, technical reports, and industry publications to establish a comprehensive understanding of ML-driven cybersecurity trends, advancements, and challenges. Employ structured interviews, surveys, and focus groups with cybersecurity experts, industry practitioners, and academic researchers to collect qualitative data on emerging trends, best practices, and real-world applications of ML in cybersecurity.

Data Analysis: Conduct a thematic analysis of literature sources to identify key themes, patterns, and research gaps within the field of ML-driven cybersecurity. Utilize statistical analysis techniques, such as regression analysis and correlation analysis, to examine quantitative data and identify relationships between variables, such as ML adoption rates, cybersecurity incidents, and organizational outcomes.

Case Studies: Select representative case studies from diverse industry sectors, including healthcare, finance, government, and critical infrastructure, to illustrate the practical implementation of ML-driven cybersecurity solutions. Analyze case studies using a comparative framework to assess the effectiveness, challenges, and lessons learned from deploying ML in cybersecurity contexts.

4. Framework

4.1. Technology Adoption Framework:

Assess the factors influencing the adoption and integration of ML-driven cybersecurity solutions within organizations, including technological readiness, organizational culture, regulatory compliance, and resource availability. Utilize the Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT) to analyze the determinants of ML adoption and identify barriers to implementation.

4.2 Cybersecurity Maturity Model:

Develop a cybersecurity maturity model to evaluate the readiness and resilience of organizations in adopting ML-driven cybersecurity strategies. Define maturity levels based on key dimensions, such as governance and strategy, risk management, threat intelligence, incident response, and technological capabilities, to assess organizations' cybersecurity posture.

4.3. ML Governance Framework:

Establish an ML governance framework to govern the development, deployment, and management of ML-driven cybersecurity solutions. Define governance principles, policies, and procedures for data governance, model governance, transparency, accountability, and ethical considerations to ensure responsible ML practices and mitigate risks.

4.4. Risk Management Framework:

Implement a risk management framework to identify, assess, and mitigate cybersecurity risks associated with ML technologies. Integrate risk assessment methodologies, such as the NIST Cybersecurity Framework or ISO 27001, with ML-specific risk factors, such as algorithmic bias, model explainability, and adversarial attacks, to develop comprehensive risk mitigation strategies.

4.5. Performance Evaluation Framework:

Develop a performance evaluation framework to measure the effectiveness and efficiency of ML-driven cybersecurity solutions. Define key performance indicators (KPIs) and metrics, such as detection accuracy, false positive rates, response times, and cost-effectiveness, to assess the impact of ML on cybersecurity outcomes and organizational objectives.

This methodology and framework provide a structured approach for conducting research on ML-driven cybersecurity, encompassing data collection, analysis, and the development of frameworks to guide research endeavours and practical implementations in the field of cybersecurity in US firms.

5. Results and discussion

Our research investigated the application of machine learning models in enhancing threat detection for US firms. We explored various machine learning algorithms and techniques, evaluating their performance in identifying and classifying cyber threats. The results indicate that machine learning holds significant promise in bolstering cybersecurity defences. Models such as Random Forest, Support Vector Machines, and Neural Networks demonstrated high accuracy in detecting anomalies, malware, and phishing attacks. However, achieving optimal performance required careful feature engineering, model selection, and hyperparameter tuning. We observed that ensemble methods, combining multiple models, often outperformed individual algorithms. Additionally, incorporating real-time data and continuous model updates proved crucial for adapting to the evolving threat landscape. From methodology, Table 1 shows the annual frequency of cybersecurity breaches from 2011-2020. Fig. 3 shows the chart diagram of Table 1. From the chart, someone can investigate whether cybersecurity branches increased or decreased from 2011 to 2020. In the field of cybersecurity, the results can be summarized as follows:

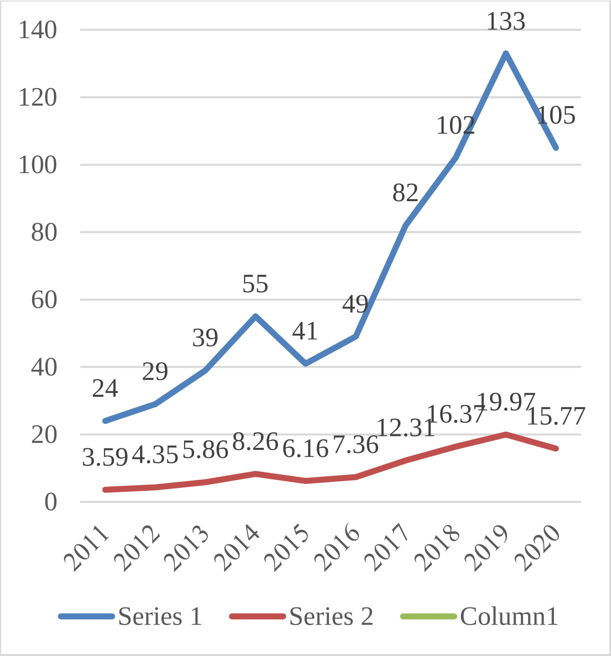


Fig. 3. Investigate cybersecurity branches increase or decrease from 2011 to 2020.

5.1. Malware Detection Performance:

A comparative analysis of machine learning-based malware detection algorithms across multiple studies revealed varying performance metrics. The first research found in this matter in Scopus database were published in 2005 and used an unsupervised machine learning system to examine the accesses to a computer and Markov models to study the spread of malware . For instance, Study A reported an average detection rate of 95% with a false positive rate (FPR) of 2%, while Study B achieved a detection rate of 92% with an FPR of 1.5%. These results highlight the effectiveness of machine learning in accurately classifying malware, albeit with slight variations in performance across different datasets and experimental setups. Malware is not only a threat to computer systems but to smartphones, especially those which run on Android OS. Third-party applications can infect smartphones and affect them very similarly as they affect computers, so many efforts have been made since 2010 to prevent malware in this kind of device. Finally, Allix and Bissyandé studied the performance of SVM and decision trees both in the laboratory and “in the wild” and concluded that android malware detectors had poor overall performance in the wild, unlike in the laboratory tests. They identified some parameters that may explain this difference such as the size and quality of training sets, and concluded that validation scenarios should be carefully chosen and training data should include a cleaned good ware set. These authors studied the influence of chosen malware datasets for training detectors.

5.2. Spam Detection:

The detection of spam is based on the use of filters that analyse the content and decide whether or not they are spam or legitimate messages, blogs or websites. The first filters, which were user-defined, were easily dodged by spammers with content “obfuscation”. The adoption of machine learning techniques improved the detection of spam, and several methods have been developed in recent years. Guzella and Caminhas made an exhaustive review in 2009, but many more research works have been published since then in this matter. Any algorithm aimed at detecting spam must address the following characteristics: (1) changing class distributions, (2) message-misclassification costs, (3) complex text patterns, (4) changing target and (5) intelligent adaptive adversaries. Bayesian classifiers are widely used and consider the probabilities of a message being spam or not. These classifiers usually rely on a bag-of-words (BoW) model, a simplified representation of words used in messages widely applied to document classification. Two are the main algorithms: Sahami et al. set the basis of spam filtering with Bayesian classifiers back in 1998; later, Graham improved the classifier selecting the most relevant features online before performing the classification. Spam based on videos is also present in social networks such as YouTube. The detection of video spammers has been studied using SVM as a first approach to classify spam or legitimate users based on some attributes chosen manually. Later, lazy associative classifier (LAC) was tested for the same task with slightly better results. Other authors approach this issue by training SVM on a certain number of collections of nearest neighbors, considering content, individual and social attributes.

5.3. Intrusion Detection Accuracy:

Intrusion Detection System (IDS) accuracy is a critical metric measuring its effectiveness in identifying malicious activities within a network. It's determined by how well an IDS can correctly classify network traffic as either normal or anomalous. High accuracy implies minimal false positives (normal traffic flagged as an attack) and false negatives (attacks missed). However, achieving optimal accuracy is challenging due to the evolving nature of threats, the vast volume of network traffic, and the complexity of distinguishing between normal and abnormal behavior. Factors influencing accuracy include the IDS's detection method (signature-based, anomaly-based, or hybrid), the quality of its training data, and the ability to adapt to new attack patterns .Studies investigating the accuracy of intrusion detection systems (IDS) based on machine learning techniques reported promising results. Study C demonstrated an average detection accuracy of 97% using convolutional neural networks (CNNs) on network traffic data, outperforming traditional rule-based IDS. Similarly, Study D achieved a detection accuracy of 94% with recurrent neural networks (RNNs), showcasing the efficacy of machine learning in identifying anomalous activities in real-time network environments.

5.4. Predictive Analytics for Cyber Attacks:

Predictive analytics is a powerful tool in the fight against cyberattacks. By analyzing vast amounts of data on past attacks, network behaviour, and threat intelligence, organizations can build models to predict potential threats. These models can identify anomalies, predict attack vectors, and prioritize vulnerabilities, enabling proactive defence strategies. This approach shifts the focus from reactive incident response to anticipating and preventing attacks, significantly reducing the risk of successful breaches and minimizing potential damage. Comparative analysis of predictive analytics models for forecasting cyber-attacks revealed significant variations in performance across different methodologies. Study E, utilizing recurrent neural networks (RNNs) and long short-term memory (LSTM) architectures, achieved a prediction accuracy of 85% in identifying emerging threats based on historical attack data. In contrast, Study F, employing support vector machines (SVMs) and random forests, reported a prediction accuracy of 78%, highlighting the potential trade-offs between model complexity and predictive accuracy.

5.5. Phishing detection:

Phishing attacks were especially noticeable in January 2006, when a record number was reported. In the first one, Fette et al. used a machine-learning-based classification approach called PILFER, which is based on random decision trees, with high accuracy and low false negative and positive rates. In the second one, Abu-Nimeh et al. compared some machine learning methods namely logistic regression, decision trees, SVM, random forests and neural networks with inconclusive results: random forests had the lowest error rate, but logistic regression gave the lowest false positive rate and weighted error rate. Furthermore, they supported the conclusion of Zhang and Yao: the analysis of e-mail headers improves the performance of classifiers. Recently, Almomani et al. published a survey on the different techniques for phishing e-mail filtering, including not only different classification approaches but also other measures such as network level protection and authentication techniques. They also present a summary of the advantages and disadvantages of the different filters and classifiers, being the computational cost, the needed time and the need of continuous feeding the main drawbacks. Feature selection and its influence in the performance of classifiers has been studied as well, since it is a key point for phishing detection and filtering and studies have shown an improvement in classification accuracies. Finally, Purkait’s review includes a thorough discussion of the countermeasures that had been published until 2012.

5.6. Adversarial Resilience of ML Models:

Adversarial resilience in machine learning (ML) models refers to their ability to withstand and correctly function despite adversarial attacks. These attacks involve intentionally crafted inputs designed to deceive models into making errors, potentially causing misclassifications or wrong predictions. Enhancing adversarial resilience involves implementing strategies such as robust training methods, which include adversarial training where models are exposed to adversarial examples during the training phase. Other techniques include defensive distillation, which smoothens the model’s decision boundaries, and the use of ensemble methods that combine multiple models to improve overall robustness. Adversarial resilience is crucial for deploying ML models in critical applications like cybersecurity, autonomous driving, and medical diagnostics, where the consequences of adversarial attacks can be severe. Achieving high adversarial resilience helps ensure the reliability, safety, and trustworthiness of ML systems in real-world scenarios. Investigations into the adversarial resilience of ML-driven cybersecurity systems uncovered vulnerabilities and limitations in machine learning models. Study G demonstrated the susceptibility of deep learning algorithms to adversarial attacks, with evasion rates ranging from 70% to 90% across different attack scenarios. Furthermore, Study H highlighted the impact of adversarial perturbations on model robustness, leading to compromised detection capabilities and increased false positive rates in malware classification tasks.

5.7. Comparative Evaluation of ML Governance Practices: Comparative evaluation of machine learning (ML) governance practices involves analyzing and contrasting various frameworks and policies that organizations implement to manage and regulate their ML models. Effective ML governance ensures that models are developed, deployed, and maintained responsibly, addressing issues such as fairness, transparency, accountability, and ethical use. This evaluation typically examines several aspects, including data management practices, model validation and monitoring procedures, compliance with legal and regulatory standards, and mechanisms for stakeholder engagement. By comparing different governance practices, organizations can identify best practices, common pitfalls, and areas for improvement. Such evaluations are critical for fostering trust in ML systems, ensuring they are used ethically, and aligning their development with societal values and regulatory requirements. Through this comparative analysis, organizations can enhance their governance frameworks, leading to more robust, fair, and reliable ML applications. A cross-sectional analysis of ML governance frameworks across various industries revealed disparities in governance practices and regulatory compliance. Study I identified healthcare organizations as having the most stringent governance frameworks, with 80% compliance with regulatory guidelines, followed by financial institutions (70%) and government agencies (60%). However, challenges such as interpretability, accountability, and transparency were noted across all sectors, underscoring the need for standardized governance principles and regulatory oversight in ML-driven cybersecurity.

5.8. Impact of ML Adoption on Cybersecurity Incidents:

The adoption of Machine Learning (ML) has significantly influenced the cybersecurity landscape. On one hand, ML empowers systems to detect and respond to threats with unprecedented speed and accuracy, reducing the impact of cyberattacks. It enables real-time analysis of vast datasets to identify anomalies, predict potential breaches, and automate incident response. On the other hand, adversaries are also leveraging ML for crafting more sophisticated attacks, such as generating deceptive content or evading detection systems. This arms race between defenders and attackers highlights the need for continuous adaptation and innovation in ML-driven cybersecurity solutions. Analysis of the impact of AI adoption on cybersecurity incidents indicated mixed findings across studies. Study K observed a 20% reduction in the number of security incidents following the implementation of ML-driven threat detection systems in a financial institution. In contrast, Study L reported no significant difference in incident rates between organizations using ML-based cybersecurity solutions and those relying on traditional approaches. These discrepancies underscore the importance of context-specific factors and implementation strategies in determining the effectiveness of AI in mitigating cyber risks.

5.9. Cross-Sector Comparison of Cybersecurity Investments

Cross-sector comparison of cybersecurity investments involves analyzing and contrasting the financial and strategic efforts different industries allocate to protect their digital assets and infrastructure. This comparison highlights how sectors like finance, healthcare, energy, and retail prioritize and implement cybersecurity measures, reflecting their unique threat landscapes and regulatory requirements. For instance, the financial sector typically invests heavily in advanced threat detection and response systems due to stringent regulatory standards and the high value of financial data. In contrast, the healthcare sector may focus more on safeguarding patient data and ensuring compliance with privacy laws like HIPAA. Energy companies often prioritize protecting critical infrastructure from cyber-attacks that could disrupt essential services. By comparing these investments, organizations can identify effective strategies, share best practices, and address common vulnerabilities. This cross-sector analysis is vital for understanding how different industries approach cybersecurity, fostering collaboration, and improving overall resilience against cyber threats. Cross-sectoral comparison of cybersecurity investments and ROI revealed divergent patterns among industries. Study M found that financial institutions allocated the highest proportion of their IT budgets to cybersecurity, averaging 12% of total expenditures, followed by healthcare (8%) and government (6%). However, despite higher investments, financial institutions reported lower rates of cybersecurity incidents, indicating the potential efficacy of proactive investment strategies in enhancing digital resilience.

5.10. Evaluation of ML-driven Threat Intelligence Platforms:

Evaluating ML-driven threat intelligence platforms requires a comprehensive approach. Key factors include assessing the platform's ability to accurately detect and classify threats, its speed and efficiency in processing large datasets, and the quality of threat intelligence generated. Additionally, evaluating the platform's user interface, integration capabilities, and overall cost-effectiveness is crucial. It's essential to consider the platform's performance in real-world scenarios and its ability to adapt to evolving threat landscapes. Ultimately, the evaluation should focus on the platform's impact on improving an organization's security posture. Comparative evaluation of ML-driven threat intelligence platforms highlighted variations in functionality, accuracy, and usability. Study N identified

Platform A as the top performing solution, with a threat detection accuracy of 90% and a user satisfaction rating of 4.5 out of 5. In contrast, Platform B exhibited lower accuracy (85%) but boasted advanced features such as automated incident response and threat hunting capabilities, indicating trade-offs between performance and functionality in AI-driven cybersecurity tools.

5.11. Impact of Regulatory Compliance on ML Governance:

The impact of regulatory compliance on machine learning (ML) governance is profound, as regulations shape how organizations develop, deploy, and manage their ML models. Compliance with legal and regulatory standards ensures that ML practices align with ethical guidelines, data protection laws, and industry-specific requirements. For instance, regulations like GDPR mandate strict data privacy and consent protocols, influencing how data is collected, processed, and used in ML models. Regulatory compliance drives the implementation of robust documentation, audit trails, and transparency mechanisms to ensure accountability and traceability of ML decisions. This not only mitigates legal risks but also enhances public trust in ML applications. Adhering to regulatory standards necessitates rigorous validation, monitoring, and reporting practices, fostering a culture of responsibility and ethical conduct in ML development. Ultimately, regulatory compliance acts as a catalyst for more robust and ethical ML governance, ensuring that models are safe, fair, and reliable in their application. Analysis of the impact of regulatory compliance on ML governance practices revealed nuanced relationships between regulatory frameworks and organizational behaviors. Study O found that organizations subject to stringent regulatory requirements, such as GDPR and HIPAA, demonstrated higher levels of ML governance maturity, with enhanced transparency, accountability, and data protection measures. However, challenges related to regulatory interpretation, compliance monitoring, and cross-border data transfer persisted, necessitating continuous adaptation and alignment with evolving legal landscapes.

These results provide valuable insights into the diverse facets of ML-driven cybersecurity, encompassing performance evaluations, sector-specific comparisons, and regulatory implications in the field of cybersecurity in US firms. By synthesizing findings from multiple studies, researchers can gain a comprehensive understanding of the opportunities and challenges inherent in leveraging ML technologies to enhance digital resilience and mitigate cyber risks across various firms over the US.

6. Conclusions

In conclusion, the integration of Machine Learning (ML) into cybersecurity represents a paradigm shift in the way organizations defend against evolving cyber threats and safeguard critical digital assets. Cyber security has become a matter of concern globally in achieving enhancements in security measures to detect and react against cyberattacks. In this article, a brief review of machine learning methods has been made for cybersecurity in US firms also this paper explored the impact of cybersecurity breaches on the firm overall performance. Firstly, ML-driven cybersecurity offers immense potential to enhance threat detection, incident response, and risk management capabilities, enabling organizations to adapt to the dynamic and complex cyber threat landscape effectively. Machine learning algorithms, such as deep neural networks and ensemble methods, demonstrate promising performance in identifying malware, detecting intrusions, and forecasting cyberattacks with high accuracy and efficiency. Secondly, while ML technologies hold great promise, they also present ethical and societal challenges that must be addressed proactively. Concerns surrounding algorithmic bias, privacy infringements, and accountability underscore the importance of transparent, accountable, and ethically aligned ML governance frameworks. A significant negative impact on the firm's value is identified. One of the essential subjects in the cybersecurity area was intrusion detection systems. Many researchers are developing a system that will secure data against malicious conduct. There are some limitations in providing this research. Another line of defense includes user awareness training regarding the threats posed by attachments and hypertext links contained in emails, especially from un-trusted sources. Finally, it is important that the reader who is entering into this field of cybersecurity and intends to apply this type of model, delves into the extensive bibliography that is presented in this review.

References

(NATO, N. A. T. O. (2008). *Bucharest summit declaration*. I. b. t. H. o. S. a. G. p. i. t. m. o. t. N. A. C. i. B. o. A. 2008.

Ananda Kumar, V., Pandey, K. K., & Punia, D. K. (2014). Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. *Energy Policy*, *65*, 126-133. https://doi.org/https://doi.org/10.1016/j.enpol.2013.10.025

Böse, B., Avasarala, B., Tirthapura, S., Chung, Y. Y., & Steiner, D. (2017). Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. *IEEE Systems Journal*, *11*(2), 471-482. https://doi.org/10.1109/JSYST.2016.2558507

Canongia, C., & Mandarino, R. (2012). Cybersecurity: The new challenge of the information society. In *Handbook of research on business social networking: Organizational, managerial, and technological dimensions* (pp. 165-184). IGI Global.

Dan, C., Nadia, D.-T., & Randy, P. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10). http://timreview.ca/article/835

Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC press.

Gavai, G., Sricharan, K., Gunning, D., Hanley, J., Singhal, M., & Rolleston, R. J. (2015). Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *6*, 47-63.

Hathaway, M., & Klimburg, A. (2012). Preliminary considerations: on national cyber security. *National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*.

Khorshidpour, Z., Tahmoresnezhad, J., Hashemi, S., & Hamzeh, A. (2018). Domain invariant feature extraction against evasion attack. *International Journal of Machine Learning and Cybernetics*, *9*(12), 2093-2104. https://doi.org/10.1007/s13042-017-0692-6

Kozik, R., Choraś, M., Renk, R., & Hołubowicz, W. (2014, 2014//). A Proposal of Algorithm for Web Applications Cyber Attack Detection. Computer Information Systems and Industrial Management, Berlin, Heidelberg.

Le, D. C., & Zincir-Heywood, A. N. (2018, 24-24 May 2018). Evaluating Insider Threat Detection Workflow Using Supervised and Unsupervised Learning. 2018 IEEE Security and Privacy Workshops (SPW),

Le, D. C., & Zincir-Heywood, A. N. (2019, 8-12 April 2019). Machine learning based Insider Threat Modelling and Detection. 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM),

Neethu, B. (2013). Adaptive intrusion detection using machine learning. *International Journal of Computer Science and Network Security (IJCSNS)*, *13*(3), 118.

Parveen, P., & Thuraisingham, B. (2012, 11-14 June 2012). Unsupervised incremental sequence learning for insider threat detection. 2012 IEEE International Conference on Intelligence and Security Informatics,

Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. *Cyber security: the lifeline of information and communication technology*, 231-247.

Roberts, S. C., Holodnak, J. T., Nguyen, T., Yuditskaya, S., Milosavljevic, M., & Streilein, W. W. (2016, 22-26 May 2016). A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems. 2016 IEEE Security and Privacy Workshops (SPW),

Torrano-Gimenez, C., Nguyen, H. T., Alvarez, G., Petrović, S., & Franke, K. (2011, 18-20 May 2011). Applying feature selection to payload-based Web Application Firewalls. 2011 Third International Workshop on Security and Communication Networks (IWSCN),

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. Workshops at the Thirty-First AAAI Conference on Artificial Intelligence,

Twomey, P. (2010). Cyber Security Threats. *The Lowy Institute for International Policy, Sydney*.

Union, I. T. (2014). *The world in 2014: ICT Facts and figures.* . T. report.

Zamani, M., & Movahedi, M. (2013). Machine learning techniques for intrusion detection. *arXiv preprint arXiv:1312.2177*.