Analyzing the Impact of Regulatory Policies on the Adoption of AI Technologies in Cybersecurity

Geeta Sandeep Nadella, Hari Gonaygunta, Priyanka P Pawar, Deepak Kumar

Abstract— **In the current digital environment, Cybersecurity is still a top priority because of the severe hazards that increasingly complex attacks pose to people, businesses, and even countries. This study provides a comprehensive analysis covering the distribution of cyberattacks, the performance of machine-learning models, and the legal frameworks controlling AI and Cybersecurity adoption. A first analysis indicates a standard distribution of cyberattacks, of which a significant fraction is hostile, underscoring the pressing requirement for effective cybersecurity defense. Further analysis of machine learning models like Multilayer Perceptron (MLP), Gaussian Naïve-Bayes, and Decision Tree-Classifiers demonstrates differing efficacies in identifying and reducing cyber threats. The Decision Tree Classifier displays high accuracy and precision, comparable performance with noteworthy recall rates is displayed by Gaussian Naive Bayes, and MLP demonstrates better training efficiency. The intricacy and significance of complete laws to reduce risks and promote responsible AI deployment are highlighted by regulatory framework analysis. The results highlight the need for cooperative efforts to create flexible, inclusive regulatory frameworks that protect the digital economy and foster innovation safely despite obstacles like regulatory gaps and international cooperation. To improve digital security and ethically utilize AI technology, governments, industry customers, and researchers may benefit significantly from this research's improved understanding of cybersecurity prospects and problems.**

***Index Terms*— Cybersecurity, AI technologies, Machine learning models, Cyberattacks, Legal frameworks, Regulatory policies**

I. INTRODUCTION

Artificial Intelligence first appeared popular in 1956, then changed to a solution applied in various fields. Machine learning was first implemented in Cybersecurity when a detection system for anomalies and other intrusions was developed in the 1990s [1]. Progress in this area is constrained by limitations related to data and computing. Artificial Intelligence has become an integral part of Cybersecurity, not just a buzzword in the business world [3]. Automation in Cybersecurity that exceeds human capabilities is directly related to the ability to mimic human behavior and thought processes.

Dr. Geeta Sandeep Nadella, University of the Cumberlands, Williamsburg, KY, USA

Dr. Hari Gonaygunta, University of the Cumberlands, Williamsburg, KY, USA.

Priyanka P Pawar, University of the Cumberlands, Williamsburg, KY, USA.

Deepak Kumar, University of the Cumberlands, Williamsburg, KY, USA.

This study demonstrates this automation's ability to identify a network security intrusion [4]. A large amount of data used in ML and additional equipment are increasingly essential for businesses since the COVID-19 epidemic accelerated the path of digital transformation. On the other hand, this increased cybercrime, putting both trustworthy companies and individuals in danger. Eian forecasts that by 2025, the potential cost of cybercrime will surpass $10.5 trillion (about $32,000 per person in the US) [5]. Businesses that rely on these technologies face issues with continuity and operations. Companies must investigate how machine learning (AI) may be used in Cybersecurity. Individuals might comprehend Artificial Intelligence's possibilities in Cybersecurity more clearly. Recognitions of advances in data science and computer science, ML, have become the most critical Type of machine learning (AI) in enterprise cybersecurity [6]. "Machine learning" is the ability of a computer to absorb and adjust to its knowledge. It is categorized as a subset [7], which focuses on building specific types of systems that can view samples and make self-judgments by examining past data.

II. LITERATURE REVIEW

The vast volumes of data corporations generate enable many machine-learning applications in cyberspace. This technique has several applications in the cybersecurity field, such as process automation, anomaly detection, and threat intelligence [8]. The association between AI and online safety remains called "Cyber-AI" [2]. These educational goals are to examine how AI affects cyber-security from an organizational perspective. The use of AI, especially machine solutions, in Cybersecurity, began cutting-edge in the late 1980s with the introduction of the detection system [9]. In the 1990s, it was replaced by the Intrusion Detection System (IDS). Limited computing resources and dirty, unstructured data temporarily halted its development. The development of AI is revolutionizing the capabilities of modern cyber defense schemes.

Owing to fast digital transformation development, the importance of the intranet, besides other forms of information and communication technologies, has increased significantly in the last few years. According to [10], companies are beginning to realize the enormous potential and value of innovative technologies such as extensive datasets, supervised learning (ML), and intelligent technologies (AI). In contrast, unshakable businesses have increased with the widespread use of Information and Communications Technology, cybercrime, intimidations, and susceptibilities that touch both individuals. Today's companies rely heavily on technology, so cyber threats and attacks can negatively impact their day-to-day operations and business continuity. Since February 2020, cyberspace-related crimes have increased [11].

Organizations that store government data include the Federal Data Security and Administration Act (FISMA), which requires authorities and institutions to continuously monitor authorized FISMA systems to identify potential deficiencies based on the assessment [12]. This requirement was established by the Board of Governors of the Federal Reserve System. Any changes should be documented in the System Privacy and Security Plan (SSPP). Constant surveillance will allow agencies to respond quickly to security issues or data breaches [13]. By implementing concepts such as continuous assessment and mitigation or continuous approval, CMS hopes to improve its approach to continuous monitoring Financial Crimes Enforcement Network 2023:

Cyber security measures are implemented through the Bank Confidentiality Act (BSA) and anti-money laundering (AML) legislation to combat financial crimes. Criminals traditionally use money laundering techniques to hide or "clean up" sources of money obtained through theft or fraud. Money laundering poses serious threats to the security and stability of the US financial system [14]. The security of the country is more at risk as terrorists now use money laundering techniques to fund their business activities. Bankers are crucial in assisting authorities or prosecutors in locating illicit financial organizations and enabling actions [15].

US Federal Reserve Board of Governors, 2023: Securities and Exchange Commission Regulation Protects investor information and requires cybersecurity requirements to ensure that brokerage firms, transfer agents, registered expense advisors, and broker-dealers — collectively referred to as "covered entities" —prevent unauthorized access to or use of customer information [16]. The proposal will require them to establish written policies and procedures. Work with events. With a few exceptions, the proposed changes require interested organizations to notify anyone whose private user information has been or may be used without permission. According to the idea, the school under insurance must provide this notification as soon as possible, but not more than 30 days after its institution comes under insurance [17].

A recent study that examined Artificial Intelligence (AI) and human Cybersecurity in business directed wide-ranging works appraisal to determine how Artificial Intelligence affects Cybersecurity and humanoid features of info. The results suggest that human capabilities are now being enhanced with the help of Artificial Intelligence and point to potential changes as Artificial Intelligence becomes more autonomous [18]. Their research covered publications published between 2008 and 2018 and focused on no more than 12 articles in each journal. This study differs from others in that it looks at Cybersecurity in business as a whole, not just the human component.

A. Security Management System In AI

Currently investigating Information Security Management systems, also known as ISMS, for the level of risk management strategy [19]. For this study, An anonymized internet poll was used to gather feedback from 27 companies about operational information safety and risk control. The study focuses on data security management, and analysis methods include documentation artifacts, standard operating procedures, stakeholder engagement patterns, tools types, and data collection procedures. The Cyber Physiological Systems (also known as the ecology aim at building a structure for IoT, which can be utilized for study and instruction in several domains linked to CPS with the Web of Things [20]. The key goal involves providing actual drawings of buildings so that students and scholars Report Phrase may observe potential applications in reality.

Colleagues are considering the possibility of the firm going bankrupt in the future, and if so, following [20] how the need for an extensible Business Reporting Language (XBRL) was discussed. The aim is to learn more about how this critical transparency measure impacts the economy. According to the researchers, who used a supposedly changeable smile instead of an initial estimate of accident rates, XBRL reduced the risk of an expected accident. The study also found that companies with less open accounting practices, more volatile results, and different analyst predictions were more negatively affected. These issues also affect the methodology used in cyber-digit manufacturing. According to [21], a meta-architecture can solve this problem. This study questions the perceived cybersecurity threat in banking with the help of a browser instrument shaped by manufacturing and scheme engineers. Utilizing the Uncertain Evaluator by way of the suitability worth, Genetic Algorithms (GA) are used to select the sequence of elements of the defense mechanism. The result of this process is an idea.

B. Application In Cybersecurity

Applications of AI in Cybersecurity offer a revolutionary way to deal with the dynamic environment of cyber threats and assaults. Beyond the limitations of conventional rule-based systems, AI technologies have capabilities that enable more proactive and adaptable protection mechanisms [22]. Identifying and responding to threats is one of the main uses of AI in Cybersecurity. Large volumes of data, such as system logs, user activity, and network traffic, might remain examined through machine learning systems to find unusual designs pointing to future cyberattacks. Artificial Intelligence (AI)-powered systems may improve detection accuracy and decrease f-positives by repeatedly seeking new information and reacting to developing threats, helping companies respond quickly to security problems [23].

Figure 1. AI application of Cybersecurity

• Faster detection: is a crucial component of Cybersecurity, and AI technologies shine in this area by making it possible to identify such risks quickly. Using machine learning algorithms, AI can examine enormous

amounts of statistics, such as system logs, network traffic, and user activity [6]. These algorithms may then identify unusual patterns that may be signs of cyberattacks. With this feature, enterprises can quickly detect and address security issues, limiting the time threats remain on their networks and the likelihood of data breaches and service interruptions.

• Network security: is essential for protecting against various online risks, including malware infestation and unwanted access attempts. Because AI has sophisticated threat detection capabilities, it is essential for improving network security. AI-powered network security solutions can detect suspicious activity and possible vulnerabilities using deep learning algorithms and anomaly detection techniques [2]. This enables enterprises to proactively strengthen network defenses and stop illegal access or data exfiltration.

• Phishing detection: is a big problem for businesses since phishing attempts are becoming more frequent and sophisticated. By using Natural Language Processing (NLP) algorithms to evaluate email content and identify phishing attempts, Artificial Intelligence (AI) technologies provide efficient ways to counteract phishing attacks [24]. AI-powered phishing detection systems can assist organizations in blocking malicious emails before they reach their intended recipients, lowering the risk of credential theft, malware infections, and other cyberattacks. These systems identify suspicious patterns, such as deceptive language or spoofed sender addresses.

• Secure and prevention: A strong cybersecurity plan must include measures, and AI helps businesses improve their security posture by taking preventative action. Predictive analytics is a tool that AI-driven security systems may use to foresee possible security risks and vulnerabilities [25]. This enables businesses to proactively put preventative measures in place and mitigate prospective threats before they become real. Furthermore, AI-powered security systems can constantly change and adapt to new threats, protecting enterprises against dynamic threat landscapes and cyberattacks.

• Behavioral analytics: an effective tool for identifying and addressing unwanted activity on a network within a business and insider threats. Artificial Intelligence (AI)-driven behavioral analytics systems can detect and identify anomalies in user behavior, which may be signs of insider threats, compromised accounts, or criminal activity [26]. By using this feature, businesses may lessen the chance of insider attacks, data breaches, and compliance infractions by proactively identifying and mitigating internal security threats.

AI is essential for improving security posture since it can do risk assessment and predictive analytics. Artificial Intelligence (AI)-powered solutions may assist enterprises in managing resource allocation and security measure prioritization by evaluating previous data and spotting trends of vulnerabilities and attack vectors [21]. Additionally, AI-driven risk assessment frameworks may offer proactive suggestions for reducing possible security threats, allowing businesses to anticipate and take preventative action.

III. METHODOLOGY

This process begins with importing libraries (such as Panda, Numpi, Marine, and SkateLearn) necessary to process, visualize, and model data. The UNSW_NB15 dataset is then loaded, and its integrity is checked to ensure consistency between the training and testing sets [27]. This dataset was selected because of its importance to intrusion detection systems (IDS). There are no duplicate records or missing values in the dataset. A visual assessment of the distribution of attack types indicates a slight class imbalance that supports general data. Using feature engineering methods, remove external columns and encode categories using a label encoder. Features that are strongly correlated are found and eliminated to solve multicollinearity. After dividing the dataset into train and test sets in a 70/30 ratio, the standard scalar is used to apply feature scaling data to standardize datasets. This data is used to train and evaluate various machine-learning models, decision tree classifiers, simple Gaussian Bayesian algorithms, and multilayer perceptron neural networks (MLPs).

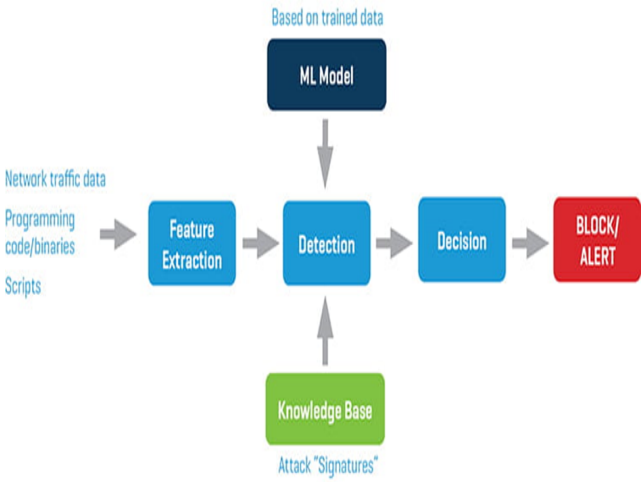

Figure 2: Proposed Framework

A. Data collections

Acquiring the UNSW_NB15 dataset, which serves as the basis of this study on Intrusion Detection Systems (IDS), was a step in the data-gathering process. The selection of the dataset was based on its wide coverage of network traffic data, which is crucial for training and assessing intrusion detection systems [28]. It has many characteristics, such as attack categories, packet and byte counts, network protocol, and service types. There is a training set and a testing set in the dataset obtained from an internet source. After the dataset was retrieved, its integrity was verified by looking for duplicate entries and missing values, which were discovered to be absent. Comprehending the class prevalence within the dataset, the distribution of assault types was also examined. This dataset is critical in developing and evaluating effective intrusion detection models to safeguard network security.

B. Feature Extractions

Several preprocessing procedures were used during the feature extraction phase to prepare the data for model training. At first, columns that were regarded superfluous for binary classification—such as the identity column ('id') and assault category ('attack_cat')—were eliminated [29].

LabelEncoder was used to encode categorical characteristics, such as "proto," "service," and "state," into a numerical representation that made modeling easier. To further ensure that the characteristics in the dataset are independent of one another and to reduce multicollinearity, strongly correlated features were found and eliminated. This stage included looking at the correlation matrix to eliminate characteristics with a correlation coefficient higher than 0.85. After preprocessing, the dataset was split into features (X) and labels (y). StandardScaler was used to apply feature scaling, which standardized the feature values' range. These preprocessing steps are crucial for enhancing the performance and interpretability of machine learning models trained on the dataset [30].

C. Implement Machine Learning Models

Three distinct methods were A Naive Gaussian Bayes, a decision-tree classification algorithm, and Multilayer Perceptron [MLP], three methods utilized in developing predictive models.

• Using Bayes naive & D-Tree Classifier models were trained using the scikit-learning package. The process of decision-making Classifier is a popular method for classification jobs that iteratively splits the data based on features to increase the accuracy of every split, creating a tree-like structure [31]. Given probability classification, Gauss Naive Bayes calculates the probability of every label for each class that provides the characteristic data. It is predicated on features independent and the Bayesian hypothesis.

• TensorFlow and Keras were used to create the Multilayer Perceptron (MLP) model, a kind of artificial neural network. Multiple layers of nodes make up MLPs. Each node applies a start purpose toward its biased amount of contributions, allowing MLPs to model complex nonlinear relationships in the data [32]. The implemented MLP architecture included an activated sigmoid in the resultant level, enabling binary categorization after several layers of density with Relearning functions that activate.

Applying the model to the training data using the fit() method and assessing its performance on the test set comprised the training process for each model. The recall, accuracy, and precision measures were calculated to evaluate how well the model classified normal behavior and attack cases. In order to compare the computing efficiency of each model, training time was also measured [33]. These various machine learning algorithms offer a thorough assessment of their effectiveness in intrusion detection, assisting in creating reliable and precise intrusion detection systems.

D. Cyber Detection and Evolutions

Cyberattack detection and mitigation strategies are increasingly important to protect digital infrastructure from evolving threats. Using machine learning models is essential to identify and prevent cyberattacks [32]. The core motivation of our examination was implementing three well-known machine learning algorithms for intrusion detection: decision tree classifiers, Gaussian navigations, and Multilayer Perceptrons (MLPs). The below Figure 3 shows how cyber attacks are distributed in the dataset, where the label "0" indicates common cases and "1" indicates attacks. More precisely, the dataset includes 800,000 incidents of common occurrence, but 160,000 incidents of cyber attacks are significantly smaller.

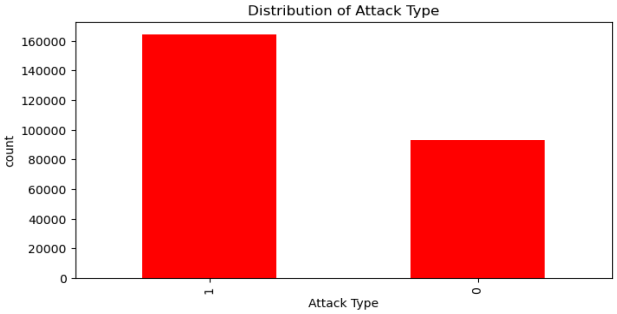

Figure 3: Cyber Attacks Distribution

This distribution shows a significant class imbalance with a 5:1 ratio between the number of standard and aggressive cases. This class imbalance is common in real-world cybersecurity datasets, where hostile actions are relatively low compared to regular network traffic [28]. The performance of three machine learning algorithms, Decision Tree Classifier, Gaussian Naive Bayes, and Multilayer Perceptron (MLP), was evaluated for cyber intrusion detection, with results summarized in the table below.

Table 1: Models results Comparison

Model	Trainings Score	Accuracy	Precision	Recall	Trainings Time
D-Trees Classifier	0.993513	0.926496	0.944833	0.940139	3.070201
Gauss-Naive Bayes	0.822871	0.823213	0.847071	0.883510	0.102164
MLP	0.924737	0.924737	0.941750	0.940685	302.658935

With a training score of 0.993513, the Decision Tree Classifier demonstrated the highest skill level in learning from the training set. With an accuracy of 0.926496, it could have correctly categorized 92.65% of the cases. With precision and recall scores of 0.944833 and 0.940139, respectively, it could distinguish between malicious and legitimate network traffic [27]. However, at 3.070201 seconds, this model's training time was comparatively longer than the others. On the other hand, the Gaussian Naive Bayes model had a similar accuracy of 0.823213 but a lower training score of 0.822871. Its recall score of 0.883510 was greater than the Decision Tree Classifier's despite its somewhat lower precision score (0.847071). Gaussian Naive Bayes had the shortest training time among the models, completing training in just 0.102164 seconds.

IV. IMPACT OF REGULATORY POLICIES IN CYBERSECURITY

Examining the legal frameworks controlling Cybersecurity and the use of AI reveals a complicated environment influenced by several variables, such as dangers that are always changing, geopolitical concerns, and technical developments. Fundamentally, these legal frameworks aim to protect private information, private infrastructure, and

sensitive data from cyberattacks while promoting the ethical use of AI.

A. POLICIES INVOLVED

Section 1. Purpose. Acknowledging Artificial Intelligence's (AI) enormous promise and related risks is critical. Using AI responsibly can significantly increase global security, wealth, productivity, creativity, and ability to handle pressing crises [34]. Meanwhile, careless usage might exacerbate problems like fake news, bias, discrimination, and fraud; it could also hurt workers by stealing their jobs and power, stifling competition, and even endangering our national security. We need to figure out how to reduce the hazards associated with AI if we are to take advantage of its many benefits and apply it for good. All social levels, including the public and business sectors, academic institutions, and civic groups, must work together on this project.

Section 2. Principles and Policies: The government will be guided by eight basic objectives and guidelines for promoting and monitoring the research and application of artificial Intelligence [35]. According to legislation and other important issues, including other agencies, companies, educational institutions, civil society, trade unions, international partners, and other relevant groups, executive departments and agencies (agencies) are required to follow these principles while performing the duties listed in this order:

a) Artificial Intelligence requires protection and security. To achieve this goal, systematic, reproducible, reliable, and standardized assessments of AI institutions, regulations, and systems also need a process to identify, understand, and mitigate the risks associated with these technologies before they can be implemented [36]. In addition to addressing the most critical security concerns of artificial intelligence systems, such as biotechnology, Cybersecurity, critical infrastructure, and other threats to national security, it also calls for limiting the transparency and complexity of Artificial Intelligence.
b) The United States can maintain its position as a global leader in artificial Intelligence while recognizing technology's ability to solve some of society's most pressing problems by encouraging ethical innovation, healthy competition, and cooperation [37]. To achieve this goal, we must help solve research, development, education, and capacity-building issues and emerging problems in Artificial Intelligence (AI) and other related Intellectual Property (IP) issues. To ensure that the United States continues to play a leading role in cutting-edge technology and business innovation, the Administration will support several initiatives designed to prepare the next generation of Americans to work in artificial Intelligence (AI) and to attract the brightest minds in the field to study and work in the United States.
c) The Administration's commitment to promoting equality and civil rights in the field of AI policy should be taken into account. The use of artificial Intelligence to discriminate against those who are mistreated is unacceptable to the government. Several sectors, including healthcare, housing, and employment, have explored what happens when artificial Intelligence encourages prejudice and discrimination rather than improving people's lives [35]. The reckless adoption of artificial Intelligence has given rise to new forms of discrimination, caused further harm both offline and online, and exacerbated and perpetuated pre-existing inequalities.
d) The federal government should monitor, regulate, and encourage appropriate intelligence usage and manage technology-related dangers to improve Americans' lives and start with people because they are the most valuable resource in our country [38]. The Administration's main objective is to find, hire, and train artificial intelligence professionals committed to working for the public good in technology, policy, governance, procurement, regulation, ethics, governance, and law. We will also make it easier for experts in this field to work for the federal government so that artificial Intelligence can be appropriately used and regulated.

B. Interdependency of Cyber Security and Artificial Intelligence

Artificial Intelligence and cyber-securities are increasingly interconnected. This area includes creating and implementing artificial intelligence-based cyberattacks, Cybersecurity for artificial intelligence systems, and AI-based counterattack systems. The three main applications of AI in Cybersecurity examined in the study are Cybersecurity to protect artificial Intelligence from potential vulnerabilities, Cybersecurity to help or enhance artificial intelligence capabilities, and the criminal use of Artificial Intelligence to carry out cyber-attacks [36]. AI can recover Cybersecurity by automating time-consuming processes, including email analysis, network threat detection, and malware classification. Many artificial intelligence systems have already been commercially deployed. Active/compatible firewalls and smart forensics are two examples of existing security methods that need to be improved.

The malicious use of artificial Intelligence has also increased. Botnets controlled by artificial Intelligence were successfully used to attack online marketplaces, and deep faxes developed using generative adversarial networks were successfully used in complex projects. The potential for adaptive cyberattacks that can learn to evade detection is real, and their use is expected to grow. Something like the Covid epidemic could happen: AI-powered bots could hijack weak internet accounts and spread misleading information. It can then be extended to include password cracking through DDoS attacks and artificial Intelligence

[39]. The malicious use of artificial Intelligence has also increased. Botnets controlled by artificial Intelligence were successfully used to attack online marketplaces, and deep faxes developed using generative adversarial networks were successfully used in complex projects. The potential for adaptive cyberattacks that can learn to evade detection is accurate, and their use is expected to grow. Something like the Covid epidemic could happen: AI-powered bots could hijack weak internet accounts and spread misleading information. It can then be extended to include password cracking through DDoS attacks and artificial Intelligence. Artificial Intelligence (AI) simplifies the operational process and improves overall convenience, which plays a role in monitoring Cybersecurity [40].

Powered by AI, job automation is viewed as an answer since people are the most vulnerable link in the safety chain. Matters because of the claim that human mistakes are the primary reason for cybersecurity vulnerabilities [41]. Eliminating human mistakes whether from a decision-based error based on skills monitoring—is the initial step towards building a safe cyber ecosystem, a mistake made in performing a desired activity. In this regard, better risk detection techniques can be helpful. The automated machine learning algorithm for the Intrusion Detection System (IDS) lets you promptly identify the most minor threats or attacks. With the help of artificial Intelligence, this process can be completed quickly rather than in hours, as happened in previous generations [42].

V. RECOMMENDATIONS

Several important recommendations have been made to improve cybersecurity defenses and encourage the appropriate usage of AI based on a thorough investigation. First and foremost, companies have to give top priority to strengthening their cyber security plans through the acquisition of cutting-edge threat detection tools and the development of solid incident response procedures. This preventative measure can lessen possible losses and the effects of cyber events. Second, machine learning models such as Multilayer Perceptron (MLP), Gaussian Naive Bayes, and Decision Tree Classifiers should be considered to supplement current security measures [42]. These models significantly increase detection accuracy and have shown promising performance in cyber threat detection. To stay on top of emerging security threats, it is also critical to constantly analyze computer logs and network usage. Companies must comply with all applicable rules and regulations and carefully manage the regulatory frameworks regulating Cybersecurity and AI deployment. Organizations reduce legal risk and increase stakeholder confidence by following rules [36, 43, 44]. These suggestions can improve cyber resilience and promote ethical AI deployment in the digital world.

VI. CONCLUSION

Cyber risks and assaults are on the rise due to enterprises integrating technology more and more. The thorough examination of the performance of machine learning models, the distribution of cyberattacks, and the legal frameworks controlling AI adoption and Cybersecurity offers important insights into how digital security is developing. The distribution of cyberattacks is examined to show how common threats are and how many are attacks rather than regular activities. This emphasizes how urgently strong cybersecurity measures are needed. Moreover, the assessment of machine learning models, such as MLP, Gaussian Naive Bayes, and Decision Tree Classifier, shows differing levels of efficacy in identifying and reducing cyber risks. The Decision Tree Classifier has exceptional precision and accuracy, although the Gaussian Naive Bayes performs competitively and has noteworthy recall rates. MLP performs better during training time than both models, although it is somewhat less accurate. Furthermore, examining regulatory frameworks highlights a nuanced but critical component of Cybersecurity and AI adoption, highlighting the necessity of strong rules to reduce risks and guarantee responsible innovation. The results highlight the need for ongoing adaptation and cooperation to handle changing cyber threats and safely utilize the potential of AI technology despite obstacles like legislative gaps and international coordination. It is essential to take a comprehensive strategy, integrating government, business, academic institutions, and civil society partners, to create flexible and inclusive regulatory frameworks that preserve digital infrastructure, uphold individual rights, and promote innovation. Considering factors like the need for stricter regulations and the absence of comprehensive AI-based solutions is crucial.

REFERENCES

[1] Natale, S., & Ballatore, A. (2020). Imagining the thinking machine: Technological myths and the rise of artificial Intelligence. Convergence, 26(1), 3-18.

[2] N.N. Abbas, T. Ahmed, S.H.U. Shah, M. Omar, H.W. Park Investigating the applications of artificial Intelligence in cyber security Scientometrics, 121 (2) (2019), pp. 1189-1211

[3] Kaplan, M. Haenlein Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence Business Horizons, 62 (1) (2019), pp. 15-25

[4] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, …, K.K.R. Choo Artificial intelligence in cyber security: Research advances, challenges, and opportunities Artificial Intelligence Review (2021), pp. 1-25

[5] I.C. Eian, L.K. Yong, M.Y.X. Li, YH Qi, Z. Fatima Cyber-attacks in the era of COVID-19 and possible solution domains (2020)

[6] J. Scott, M. Kyobe Trends in cybersecurity management issues related to human behaviour and machine learning 2021 International Conference on Electrical, computer and energy technologies (ICECET), IEEE (2021), pp. 1-8

[7] M. Wazid, A.K. Das, V. Chamola, Y. Park Uniting cyber security and machine learning: Advantages, challenges and future research ICT express, Korean Institute of Communication Sciences (2022), pp. 313-321, 10.1016/j.icte.2022.04.007

[8] M.H. Huang, R.T. Rust Artificial intelligence in service Journal of Service Research, 21 (2) (2018), pp. 155-172

[9] Prasad, R., & Rohokale, V. (2020). Cyber security: the lifeline of information and communication technology. Cham, Switzerland: Springer International Publishing.

[10] F. Almeida, J.D. Santos, J.A. Monteiro The challenges and opportunities in the digitalization of companies in a post-COVID-19 World IEEE Engineering Management Review, 48 (3) (2020), pp. 97-103

[11] F. Almeida, J.D. Santos, J.A. Monteiro The challenges and opportunities in the digitalization of companies in a post-COVID-19

World IEEE Engineering Management Review, 48 (3) (2020), pp. 97-103
[12] Gillis, A. S. (2020). Federal Information Security Management Act (FISMA). Tech Target. September.
[13] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.
[14] Ciarabellini, J. (2020). Cryptocurrencies' Revolt against the BSA: Why the Supreme Court Should Hold That the Bank Secrecy Act Violates the Fourth Amendment. Seattle J. Tech. Envtl. & Innovation L., 10, 135.
[15] Zagaris, B., & Adhoob, M. (2021). Money Laundering, Bank Secrecy and Financial Confidentiality. IELR, 37, 454.
[16] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of Cybersecurity. Sustainability, 15(18), 13369.
[17] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.
[18] Jada, I., & Mayayise, T. O. (2023). The impact of artificial Intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 100063.
[19] Brunner, M.; Sauerwein, C.; Felderer, M.; Breu, R. Risk management practices in information security: Exploring the status quo in the DACH region. Comput. Secure. 2020, 92, 101776.
[20] Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. Journal of Network and Computer Applications, 161, 102630.
[21] Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access, 9, 23235-23263.
[22] Sarraf, A., Azhdari, M., & Sarraf, S. (2021). A comprehensive review of deep learning architectures for computer vision applications. American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), 77(1), 1-29.
[23] Crawford, K. (2021). The atlas of AI: Power, politics, and the planetary costs of artificial Intelligence. Yale University Press.
[24] Chowdhary, K., & Chowdhary, K. R. (2020). Natural language processing. Fundamentals of artificial Intelligence, 603-649.
[25] Bothe, M., Ronzitti, N., & Rosas, A. (Eds.). (2023). The OSCE in the maintenance of peace and security: Conflict prevention, crisis management and peaceful settlement of disputes. Martinus Nijhoff Publishers.
[26] Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT security for smart cities. ACM Transactions on Internet Technology, 21(4), 1-21.
[27] Zoghi, Z., & Serpen, G. (2024). UNSW□NB15 computer security dataset: Analysis through visualization. Security and Privacy, 7(1), e331.
[28] Al-Daweri, M. S., Zainol Ariffin, K. A., Abdullah, S., & Md. Senan, M. F. E. (2020). An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system. Symmetry, 12(10), 1666.
[29] Aleesa, A., Younis, M. O. H. A. M. M. E. D., Mohammed, A. A., & Sahar, N. (2021). Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques. Journal of Engineering Science and Technology, 16(1), 711-727.
[30] Kumar, V., Das, A. K., & Sinha, D. (2020). Statistical analysis of the UNSW-NB15 dataset for intrusion detection. In Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2019 (pp. 279-294). Springer Singapore.
[31] Palimkar, P., Shaw, R. N., & Ghosh, A. (2022). Machine learning technique to prognosis diabetes disease: Random forest classifier approach. In Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2021 (pp. 219-244). Springer Singapore.
[32] Zhang, J., Li, C., Yin, Y., Zhang, J., & Grzegorzek, M. (2023). Applications of artificial neural networks in microorganism image analysis: a comprehensive review from conventional multilayer perceptron to popular convolutional neural network and potential visual transformer. Artificial Intelligence Review, 56(2), 1013-1070.
[33] Grattarola, D., & Alippi, C. (2021). Graph neural networks in tensorflow and keras with spektral [application notes]. IEEE Computational Intelligence Magazine, 16(1), 99-106.
[34] Abioye, S. O., Oyedele, L. O., Akanbi, L., Ajayi, A., Delgado, J. M. D., Bilal, M., ... & Ahmed, A. (2021). Artificial Intelligence in the construction industry: A review of present status, opportunities and future challenges. Journal of Building Engineering, 44, 103299.
[35] Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., ... & Zhou, B. (2023). Trustworthy ai: From principles to practices. ACM Computing Surveys, 55(9), 1-46.
[36] Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 57-69.
[37] Bhutoria, A. (2022). Personalized education and artificial Intelligence in the United States, China, and India: A systematic review using a human-in-the-loop model. Computers and Education: Artificial Intelligence, 3, 100068.
[38] Köstler, L., & Ossewaarde, R. (2022). The making of AI society: AI futures frames in German political and media discourses. AI & society, 37(1), 249-263.
[39] Khempetch, T., & Wuttidittachotti, P. (2021). DDoS attack detection using deep learning. IAES International Journal of Artificial Intelligence, 10(2), 382.
[40] Paleyes, A., Urma, R. G., & Lawrence, N. D. (2022). Challenges in deploying machine learning: a survey of case studies. ACM computing surveys, 55(6), 1-29.
[41] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science, 171, 1251-1260.
[42] Desai, M., & Shah, M. (2021). An anatomization on breast cancer detection and diagnosis employing multilayer perceptron neural network (MLP) and Convolutional neural network (CNN). Clinical eHealth, 4, 1-11.
[43] K. Meduri, "Cybersecurity threats in banking: Unsupervised fraud detection analysis," *International Journal of Science and Research Archive*, vol. 11, no. 2, pp. 915–925, Apr. 2024, doi: 10.30574/ijsra.2024.11.2.0505.
[44] K. Meduri, H. Gonaygunt, and G. S. Nadella, "Evaluating the Effectiveness of AI-Driven Frameworks in Predicting and Preventing Cyber Attacks," *International Journal of Research Publication and Reviews*, vol. 5, no. 3, pp. 6591–6595, Mar. 2024, doi: 10.55248/gengpi.5.0324.0875.

Dr. Geeta Sandeep Nadella received an MS in Information Assurance from Wilmington University in 2015 and a Ph.D. in Information Technology from the University of Cumberlands in 2023. He has over twelve years of experience as a senior quality assurance consultant and over four years of experience as a seasoned Scrum Master. He also an IEEE Senior Member and serves as an IEEE Computer Society Chair for the Eastern North Carolina Section. He has also received the Epsilon-Pi-Tau Honorary Excellence Award from Wilmington University.

Dr. Hari Gonaygunta Hari Gonaygunta received a Ph.D. in Information Technology from the University of Cumberland, Kentucky, in 2023, a master's in computer science from San Francisco Bay University, California, in 2016, and a Master in Power Systems from the National Institute of Technology, Jamshedpur, India, 2010. He is an active IEEE member, and his research interests include but are not limited to Data Science, AI, ML, IoT, Blockchain Technologies, and Cyber Security.

Dr. Priyanka P Pawar received her Master's in Computer Science from San Francisco Bay University, CA, USA, in 2016 and a Doctorate in Information Technology in 2022 from the University of the Cumberlands, KY, USA, in 2022. She is currently working as a Software Engineer in Silicon Valley for a prominent EV company.

Dr. Deepak Kumar completed an M. S in Computer Science from San Francisco Bay University, CA, USA, in 2016 and a Doctor of Philosophy in Information Technology from the University of the Cumberlands, KY, USA, in 2022. He has ten years of experience in software development, where he worked with different technologies like Java, Python, SQL, Big Data, Real-time ingestion systems, and visualization tools.