**Journal of Computer Science and Technology Studies**
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

**| RESEARCH ARTICLE**

# The Digital Shield: An Analysis of AI's Role in Protecting US Financial Infrastructure from Cyberattack

**Mohammad Kowshik Alam[1] and Md Lutfur Rahman Fahad[2]**
[1] *Master of Science in Business Analytics, Grand Canyon University, Arizona, USA*
[2] *Master of Science in Information Systems, Pacific State University, Los Angeles, USA*
**Corresponding Author:** Mohammad Kowshik Alam, **E-mail**: alammohammadkowshik@gmail.com

**| ABSTRACT**
The complexity of cyberattacks is a consistent challenge to the stability and credibility of financial institutions in the United States. Increasing vulnerability of financial systems to cyber-based criminal activities, including fraud, data breach and identity theft, has been observed as a result of the rapid pace of digital transformation. This study examines how data analytics facilitated by Artificial Intelligence (AI) can improve cybersecurity conditions in financial institutions by forecasting, identifying, and addressing possible threats on a real-time basis. I used two data sets to complete this research: the IEEE-CIS Fraud Detection dataset, which includes anonymized transactional information about the U.S. financial systems, and the Cyber Security Indexes dataset, which gives the world information about cybersecurity preparedness and the exposure. To train and test AI models of Random Forest, XGBoost, and Neural Networks, the IEEE-CIS dataset was used to find out the fraudulent transactions and test their accuracy of detection. Conversely, the dataset of Cyber Security Indexes was processed to compare the cybersecurity preparedness of the United States to the situation in other nations and investigate the relationships between cyber exposure, country preparedness, and digital development. The combined analysis reveals that AI-based models can be useful to identify fraudulent activities with high precision and recall and minimize financial loss and operational risks. The evidence shows that countries that have a better framework of cybersecurity governance and higher levels of Global Cybersecurity Index (GCI) experience less financial cybercrime exposure. This paper has reached the conclusion that AI-based analytics coupled with a strong cybersecurity framework forms a holistic protection scheme in the financial sector, which is more resilient, compliant with regulations, and trusted by the population. These findings highlight the potential of AI to transform the current state in empowering micro-level financial defenses as well as macro-level national cybersecurity infrastructures.

**| KEYWORDS**
Artificial Intelligence (AI) Cybersecurity Analytics Financial Fraud Detection Machine Learning Models Cybersecurity Readiness Indexes. U.S. Financial Institutions Defense

**ACCEPTED:** 01 June 2022 **PUBLISHED:** 25 June 2022 **DOI:** 10.32996/jcsts.2022.4.1.14

## I. Introduction

### A. *Background*

The American financial institution is at the nexus of innovation, regulation and risk in the world of hyper-connectivity of the digital economy. The advent of online and mobile banking, digital payments systems, and real-time transaction platforms have all increased to a considerable extent the amount of data that is processed in a day, as well as its speed. Although this change increases the efficiency of services to customers and also enhances customer experience, it also subjects the banking systems to more advanced cyber attacks. Such attacks can be in the form of data breach, phishing, ransomware and fraudulent transactions and they take advantage of a system vulnerability and human error [1]. Conventional rule-based cybersecurity methods have been found to be not fast enough or adaptive to such threats. As a result, data analytics driven by Artificial Intelligence (AI) has now become a disruptive technology that can analyze large volumes of transactional data and detect abnormal behavior, as well as

preempt possible intrusions in the real-time. Incorporating AI models into security systems will enable financial institutions to shift their defense to proactive threat mitigation to increase resilience and compliance with the regulations. In this regard, the combination of AI-powered analytics and predictive algorithms can provide a response mechanism, as well as strategic insights toward risk governance. Banks in the U.S are, therefore, taking advantage of machine learning and big data analytics to develop sound security designs that can withstand dynamic and emerging cyber threats [2]. The constant development of these technologies contributes to the need to address their real effectiveness and impact on the protection of financial ecosystems against complex cyber threats.

### B. *AI-driven Data Analytics and Current Cyber Defense*

The implementation of data analytics based on Artificial Intelligence has emerged as a staple of the contemporary cybersecurity defenses, especially when it comes to financial institutions, where transactions involving extensive data dealings take place on a per-second basis. AI systems have a special ability to work with complicated data, detect minor anomalies, and reveal fraud cases that would otherwise not be detected using traditional security solutions. With AI models trained with the help of supervised learning, anomaly detection, and deep neural networks, it is possible to identify the deviation in behavior and forecast the possible fraudulent criminal actions prior to the financial harm caused. In the financial industry of the U.S. where companies move trillions of dollars on a daily basis across online platforms, AI analytics can be used to enhance monitoring functions, automated risk identification, and adherence to high-level cybersecurity standards [2]. These systems have the ability to learn dynamically as well and adapt to new attack patterns, avoiding reliance on fixed rule based systems. Besides, AI-based financial cybersecurity aids in real-time memory of threats like account takeovers, unauthorized access, and high-value transaction abnormalities.[3]In addition to the benefits in the business operations, AI-based analytics can positively impact institutional transparency through the provision of explainable and auditable decision-making models, which meet the requirements of regulators and ethical standards. [4]The role of AI is examined in this paper not only using particular transaction data (IEEE-CIS Fraud Detection dataset) but also using macro-level data on cybersecurity (Cyber Security Indexes dataset). The combination of these dimensions will illustrate the fact that AI analytics does not only enhance the effectiveness of the detection of institutional-level fraud but also benefits the entire cybersecurity preparedness of the US. This combined method shows that data analysis based on AI is no longer a side-by-side tool, it is a vital part of the current cyber defense policy.

### C. *Problem Statement*

Regardless of heavy investments in cybersecurity infrastructure, the financial institutions of the U.S. are facing an ever-growing number of cyber intrusion and digital fraud cases. Some of the sophisticated strategies used by cybercriminals include social engineering, automated malware, and AI-enhanced evasion techniques that are not detected by traditional detection mechanisms [5]. This failure in updating to these dynamic threats restricts the capacity of the conventional security instruments to respond to these emerging threats in a dynamic and data-oriented manner. The lack of information integrity between the institutions makes it difficult to detect early and respond in a coordinated manner. It follows that there is an immediate requirement of research that could prove how AI-based data analytics could enhance the institutional defense mechanism by going through real time monitoring, detection of anomalies by the system, and prediction of risks [6]. This paper helps to fill this gap by assessing AI-based fraud detection models and connecting their performance with more general indicators of cybersecurity preparedness.

### D. *Objectives of the Study*

To determine how effective AI-based data analytics is in protecting American financial institutions against cybercrime and fraud.

Objectives of this studies are:

- To examine the trends of the fraudulent transactions through the AI-based predictive models.
- To assess how machine learning algorithms can be used in identifying financial cyber fraud [7].
- To determine whether there is a correlation between the national preparedness to cybersecurity and its exposure to cybercrime.
- In order to combine micro-level fraud analytics with macro-level cybersecurity index to get a complete understanding of defense.
- To present strategic suggestions to improve AI-based cybersecurity systems in the U.S. financial institutions.

### E. *Research Questions*

The research questions of this studies are below

1. What is the potential of lowering fraud detection and prevention in financial institutions in the U.S. using data analytics powered by AI?

2. What machine learning models are the most accurate and reliable when it comes to identifying cyber-enabled fraud?
3. What role does the cybersecurity preparedness of the United States shown by the international indexes play in the financial sector resilience to cyberattacks?

### F. *Significance of the Study*

This study is very relevant to the academic and practical fields. It will add to the literature on the topic of integrating artificial intelligence in cybersecurity management, which is growing. The visibility of the study is that by integrating transaction-level fraud analytics and country-level cybersecurity indicators, the study provides a dual-perspective approach to comprehend financial defense. In practice, the results will inform banks, regulating bodies, and specialists in cybersecurity to implement AI systems that increase the effectiveness of fraud detection to a minimum number of false positives [8]. The lessons learned using the IEEE-CIS Fraud Detection dataset are that the AI models like the Random Forest, XGBoost, and Neural Networks can be effectively used to predict fraudulent behavior. At the same time, the Cyber Security Indexes dataset puts such findings into context of the overall range of global cyber preparedness [9]. The findings will enable the policymakers to build coherent AI governance policy and risk management guidelines consistent with the U.S. cybersecurity policy, which will enhance national financial resilience and consumer confidence. In addition, this study can be added to the insights into the role of AI in strengthening the internal security of institutions, as well as the cyber resilience of the country in general [10]. With cyber threats undergoing an ongoing enhancement in scope and complexity, using AI-based data processing is a reactive, intelligent, and responsive method of protecting integrity of financial systems and ensuring economic confidence.

## II. Literature Review

### A. *Artificial Intelligence and Cybersecurity Development*

Artificial Intelligence (AI) has found its way into the current cybersecurity systems and has provided novel means of detecting, preventing, and responding to cyber threats. The conventional approach to cybersecurity was based on the rule-based model where the security controls were determined in advance and were fixed. Due to the emergence of advanced types of attacks, including phishing, ransomware, and zero-day attacks, these systems are no longer sufficient [11]. AI-based cybersecurity has come to this void with sophisticated algorithms that process data in bulk, detect irregularities and future attacks in real-time. With machine learning and deep learning, AI systems are able to learn on past attack trends and adapt to novel threat behaviors so that they can much more quickly identify new attacks with even greater precision. Within the financial industry, the ability of AI to work with complex transactional data can be used to detect minor fraud patterns that might be missed by a human or other non-adaptable systems. Anomaly detection techniques, clustering, and reinforcement learning are among the many techniques that are used to identify malicious activity, enhance endpoint protection, and maximize threat intelligence [12]. Also, the predictive modeling feature of AI is able to run constant surveillance and automated remedial measures that will lessen the duration of threat identification and control. Such evolution represents a paradigm shift of the current reactive cybersecurity to the intelligent, proactive, and self-learning defense frameworks. These AI systems are also used in financial institutions to secure transactions and to ensure that a transaction is compliant with the regulations and to minimize the risks of operation, thereby reinforcing the institutional and national resilience to a cyber threat.

### B. *Fintechs Involving Machine Learning Techniques in Fraud Detection*

Machine Learning (ML), which is one of the important branches of AI, is central to financial fraud detection, which is among the most common cybercrime types of financial institutions. Using ML methods allows systems to make use of the past and classify new transactions as either legitimate or fraudulent depending on the learned trends. Classification algorithms, including Logistic Regression, Decision Trees, Random Forest and XGBoost, are unsurprisingly used in most classification tasks, whereas unsupervised models like Isolation Forest and Autoencoders are used to find anomalies [13]. One of the most well known sources of training and testing such models is the IEEE-CIS Fraud Detection dataset. It has anonymized transactional information that reflects the actual reality of legitimate and fraud financial operations in the U.S. banking sector. ML models that have been trained on this data are able to have impressive levels of precision and recall and reduce false positives and detect fraudulent behavior. Deep learning approaches such as Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) are becoming popular to learn a sequence and spatial correlation in sequence of transactions. The major issue in fraud detection is the imbalance in data. One of the transactions is the fraudulent one and they constitute a small proportion of the total transactions [14]. This problem is solved with the help of oversampling techniques such as SMOTE and ensemble to make the models more robust. Explainable AI (XAI) is integrated to provide transparency, so the financial institutions can provide an explanation of the automated decisions to both the regulators and clients. It has therefore become crucial in the detection of fraud in the financial systems with ML providing adaptive intelligence that dynamically changes in accordance with the emergent fraud features and providing institutions with the ability to avoid major financial and reputation damages.

### C. *Governance and Regulatory Frameworks of Cybersecurity*

Technological safeguards cannot possibly cover complete protection against cyber threats in the absence of strong governance and control systems. Financial cybersecurity in the United States is regulated by such regulatory agencies as the Federal Financial Institutions Examination Council (FFIEC), Financial Industry Regulatory Authority (FINRA) and National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework offers a conceptual framework to identify, protect, detect, respond to and recover cyber incidents. Financial regulations put in place governance structures that focus on risk management, compliance and accountability as a way of upholding trust in the system. Additionally, the growing adoption process of AI-based security systems as analytics requires robust ethical and legal regulation to help reduce the risks associated with information privacy, bias of models, and transparency of algorithms [15]. The institutions must make sure that AI models are also in line with the standards like the General Data Protection Regulation (GDPR) and U.S. Federal Data Strategy of secure and ethical use of data. Co-operation between government and financial institutions is a very important aspect of governance as well. Through the threat intelligence sharing program like Financial Services Information Sharing and Analysis Center (FS-ISAC), collective defense against cyberattacks is enhanced. Governance structures have to undergo changes as cyber threats grow and enhance accountability and innovation [16]. A sound cybersecurity governance, therefore, fills in the gaps between technology, regulation and ethics to make AI-driven defense mechanisms increase security without undermining fairness and compliance. Such policy-technology congruence is part of a foundation of sustainable financial cybersecurity resiliency.

### D. *Indicators of cybersecurity Readiness and Global Index*

Cybersecurity preparedness is a factor of how a nation can respond, detect, and prevent cyber threats. In order to gauge this capacity, global bodies have come up with indexes that determine the exposure, commitment and readiness of a nation in the area of cybersecurity [17]. The data used in this study is the Cyber Security Indexes dataset which comprises four large indicators namely Cybersecurity Exposure Index (CEI), Global Cybersecurity Index (GCI), National Cybersecurity Index (NCSI), and Digital Development Level (DDL). All these indicators are aspects of cyber resilience. CEI has been used to measure exposure to cybercrime; GCI has been used to measure commitment to cybersecurity frameworks; NCSI has been used to measure readiness to manage incidents; and DDL has been used to measure digital maturity. When put together, these indicators provide an evaluation of cybersecurity posture at the macro-level. The United States has consistently been rated among the leading countries in terms of cybersecurity preparedness globally in terms of good governance, policy enabling infrastructure, and technological uptake. Digital maturity and globalized financial systems also expose a person to cyber risks. This dilemma highlights the role of ensuring that the institutional defenses are in line with national strategies [18]. This analysis uses national preparedness as a dependent variable that correlates with micro-level institutional resilience on the IEEE-CIS dataset by correlating the data in the cybersecurity index with AI models [19]. The discussion adds to the comprehension of the effect of international cybersecurity principles and regulating systems on the performance of computer-based financial protection systems. Finally, adding national readiness indicators to AI-based analytics would give a wholesome overview of cyber defense, both operationally and on a strategic level.

### E. *The AI-driven Data Analytics and its role in Financial Cyber Defense*

Data analytics that operate on the AI platform allow financial institutions to convert raw data into operational intelligence on cybersecurity [20]. Using big data systems and sophisticated algorithms, the AI systems will be able to identify unseen relationships between millions of transactional events and new trends of fraud. These systems are automated to monitor the process and this enables the process to be monitored at all times and prompt action taken against activities that are suspicious [21]. Predictive analytics and behavioural modelling detect the abnormalities in customer behaviour that point to the possible insider threats or external cyber intruders. Moreover, phishing attempts, fake communications, and text-based social engineering are detected using Natural Language Processing (NLP). Also, AI-driven real-time data visualization dashboards can assist cybercriminal professionals to prioritize alerts and effectively assign resources. Explainable AI application also makes certain that predictions can be interpreted to promote better transparency and compliance. In the case of financial institutions, AI-controlled analytics can improve both security and minimise operational expenses as it minimises manual intervention. On large data sets like the IEEE-CIS Fraud Detection data, AI models would perform better than the conventional rule-based systems to detect patterns of fraud and forecast the risk [22]. Together with the information gathered by the Cyber Security Indexes dataset, AI analytics can offer a multidimensional perspective on the role of data intelligence in cybersecurity on a national and institutional level. Thus, AI-based analytics is not only a technical empowerment, it is a strategic one that allows financial institutions to predict, forestall, and address cyber attacks with a higher degree of accuracy.

### F. *Research Gaps and Conceptual Framework*

Having said that, AI has proven to be a promising area in improving cybersecurity, but a number of research gaps exist that support the need to conduct this study [23]. To begin with, the current body of research is choosely dichotomous, examining either the institutional-level fraud detection or the analysis of national-level cybersecurity but rarely combines both of these frames into a single analytical approach. Second, the connection between the efficiency of AI models in detecting fraud and macro-level signs of readiness to cybersecurity has received little attention. Third, real and global datasets should be used to compare the

comparative studies of the role of national preparedness in institutional defense capacity [24]. Data imbalance, transparency of algorithms, and ethical governance of AI are the topics that lack research on the background of financial cybersecurity. The current work can fill these gaps since it uses the dual-data methodology (that involves the fusion of the IEEE-CIS Fraud Detection dataset (micro-level) and the Cyber Security Indexes dataset (macro-level). Based on the offered conceptual framework, AI-powered analytics is the mediating variable between data-driven fraud detection and strategic cybersecurity preparedness [25]. The framework evaluates the potential to enhance both the resilience of institutions and national cyber preparedness through AI on a simultaneous basis based on statistical correlation, machine learning modeling, and interpretive analysis. Such a combined approach can offer an overall perspective on the role AI plays in financial cybersecurity defense, and it opens the field of possible future research that can connect technical innovation and policy-based resilience.

### G. *Empirical Study*

In the article Big Data Analytics in Banking Risk Management: AI-Powered Decision Support Systems (2024) by Archana Pattabhi, the researcher conducts an empirical study to determine how artificial intelligence (AI) and big data analytics can be used to optimize the risk management processes of the banking industry. The paper underlines the combination of the AI-based Decision Support Systems (DSS) to enhance the detection of fraud, credit risk assessment, and regulatory compliance. The study shows how structured and unstructured banking data, including transaction data, customer profiles, and market behavior, can be converted into actionable intelligence to proactively manage the risks, which has been accomplished by applying machine learning and deep learning algorithms [1]. The results of the study by Pattabhi indicate that the AI models have a high potential of minimizing false alarms when it comes to fraud detection and they enhance the efficiency of operations in the credit reviews process. In addition, significant pitfalls have been outlined in the research, such as the threat of privacy invasion, the challenge of ethical issues in automated decision-making, and Explainable AI (XAI) as a solution to make algorithmic results transparent and accepted. Another contributor to the development of federated learning is also mentioned in the paper: it is a safe and distributed method of joint training of models among financial institutions. This empirical information is a strong argument in favor of using AI-based analytics to improve cyber risk management and institutional resilience in financial systems.

In the article, Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses, by Fnu Jimmy (2024), the author empirically examines how the concept of artificial intelligence (AI) can change the concept of cybersecurity strategies, in response to an emerging digital threat. The paper has found a list of the new types of risks, such as ransomware, phishing, zero-day attacks, and AI-controlled cyber attacks, as the global cyber opponents are becoming more sophisticated. A literature review and case study analysis allow Jimmy to prove that AI algorithms enhance threat detection in real-time, automatize incident response, and predictive risk mitigation in organizational ecosystems [2]. The article identifies the adoption of machine learning and deep learning models capable of dynamically evolving in response to new attack vectors and minimizing human error during cybersecurity operations, critics of the research include ethical and technical constraints, including bias in the data and model black boxes, and the misuse of AI in offensive cyber activities. The paper ends by highlighting the need to have a cross-sector partnership between policymakers, cybersecurity experts, and AI developers to enhance resilience and align ethical practices in the implementation of AI. This empirical fact demonstrates the central role of AI in updating the cybersecurity defenses against new and sophisticated threats.

In the article The Emerging Threat of AI-Driven Cyber Attacks: A Review, the authors performed a systematic review focusing on the increasing sophistication of cyberattacks that are driven by artificial intelligence (AI) (Blessing Guembe et al., 2022). In the study, 936 academic articles in various databases were analyzed, and eventually 46 articles addressing specifically the AI-based attack mechanisms were selected. The review established that 56 percent of AI-based attack methods are made in the access and penetration phase, and others in the exploitation, reconnaissance and command and control phases of the cybersecurity kill chain. The results also underscore the fact that cybercriminals are increasingly using AI to carry out intelligent, dynamically, and high-speed attacks, which are capable of circumventing the traditional rule-based security systems [4]. The research caution that current defense systems will not be able to cope with the changing nature of offensive AI any longer. As a result, the authors suggest the adoption of AI-powered cybersecurity systems with predictive analytics, self-learning, and automated response. The paper concludes that in order to be resilient, organizations (particularly financial institutions) need to invest in adaptive, AI-based defense structures that are capable of predicting, learning and countering advanced cyber threats before they become critical. This empirical fact is a strong indication that proactive AI analytics is required in the contemporary management of cybersecurity.

In Artificial Intelligence in Combating Cyber Threats in Banking and Financial Services, the author, Balaji Dhashanamoorthi (2021), presents an empirical and conceptual study of the role of artificial intelligence (AI) technologies in changing the practice of cybersecurity in the banking and financial industries. The paper discusses different AI-based applications like the detection of fraud, customer behaviour analysis and personal data protection; highlighting their value in detecting and eliminating cyber threats in real-time. The study, through the use of machine learning systems and predictive data analytics, underscores how AI systems can analyze and process large amounts of structured and unstructured financial data to identify anomalies, which could signal the existence of security breaches. Besides, the paper addresses the dual nature of AI, which is the ability to reinforce cybersecurity

frameworks and at the same time create new threats, including a breach of data privacy, model bias, and the lack of explainability. Dhashanamoorthi notes that current AI ethical design, human regulation, and effective regulation should be implemented to achieve transparency and accountability in AI financial systems [4]. The research finds that AI implementation in a banking cybersecurity system is a powerful resiliency factor against the dynamic cyber threats and a more effective risk management tool that will form the foundation of AI to build digital security environments in the future.

## III. Methodology

This study will use quantitative and analytic research design with the implementation of Artificial Intelligence (AI)-powered data analytics to detect and prevent cyberattacks in American financial institutions. Two data sets were employed, the IEEE-CIS Fraud Detection dataset to analyze transaction-level and the Cyber Security Indexes dataset to evaluate the readiness of cybersecurity in a country [26]. Preprocessing, normalization and feature engineering of data were performed and thereafter, machine learning models including Random Forest, XGBoost, and Neural Network were trained. The performance of each model was determined by accuracy, precision, recalls, F1-score, and AUC measures. The analysis model also connected micro-level fraud detection with macro-cybersecurity indicators to offer holistic data regarding the success of AI in financial defense systems.

### A. *Research Design*

This study is quantitative, analytical and experimental research design, which will determine the importance of Artificial Intelligence (AI)-based data analytics in protecting American financial institutions against cyber attacks [27]. The research combines both the micro-level analysis of transaction data and macro-level analysis of cybersecurity preparedness using two data sets that are complementary: the IEEE-CIS Fraud Detection dataset and the Cyber Security Indexes dataset. It is a descriptive and predictive approach that is intended to determine the connection between transaction anomalies and national cybersecurity resilience. This has been done using a multi-phase methodology. The initial step was concerned with data collection and pre-processing, making sure that the two sets of data are clean, standardized and can be subjected to analytical modeling [28]. The second phase was feature engineering and model development where machine learning models were trained on transaction level data (Random Forest, XGBoost, and Neural Networks) to identify fraudulent transactions. The third step involved correlation and regression as the predictors of cybersecurity readiness (Global Cybersecurity Index, National Cyber Security Index, and Cybersecurity Exposure Index) and the trends of fraud. Such a hybrid methodological design allows conducting a comprehensive research of the way AI analytics can improve the institutional and systemic defense mechanisms. It can also be used to provide multi-dimensional viewpoints, which is to connect the level of financial fraud detection performance and the level of maturity of global cybersecurity [29]. The scientific rigor, reproducibility, and transparency are guaranteed by the research design, which are fundamental to the data-driven studies in cybersecurity and finance.

### B. *Sources and description of data*

The analysis of the two publicly available and internationally recognized datasets, the IEEE-CIS Fraud Detection Dataset and the Cyber Security Indexes Dataset was used because they are relevant to the analysis of a financial cybersecurity problem. IEEE-CIS Fraud Detection Dataset is also obtained via Kaggle and includes millions of anonymous online transactions. It has the following fields: Transaction Amount, Device Type, IP Range, CardID, Email Domain, and Time of transaction as well as the binary isFraud that is fraudulent or not. Such a dataset is able to offer micro-level information on individual transaction behaviors and helps to detect fraud using machine learning [30]. The Cybersecurity Indexes Data set is published by the International Telecommunication Union (ITU) and the National Cybersecurity Index (NCSI) and is based upon the data of 193 countries that are measured in terms of various indicators: GPI (Global Proliferation Index) - national commitment to cybersecurity. NCSI (National Cybersecurity Index) the index measures the national preparedness and governance systems. CEI (Cyber security Exposure Index) – index of the susceptibility to cyber threats. DDL (Digital Development Level)- shows the level of technological and digital maturity [31]. The incorporation of these datasets facilitates a micro-level examination of the fraud behavior, and a macro-level examination of the cyber security preparedness, which makes it possible to contemplate the contribution of the AI-based analytics to financial defense measures in an integrated way. Pre-processing was done to make data sets clean, de-duplicated and normalized to have consistency in the analysis modelling.

### C. *Preprocessing and engineering of data*

Preprocessing of data was an important process to ascertain accuracy, quality, and integrity of data before the application of analytical models. With the IEEE-CIS dataset, the median imputation was used to address the missing values and one-hot encoding was applied to deal with the categorical variables [32]. Those features that had low variance were eliminated to avoid overfitting and enhance the performance of the model. The Interquartile Range (IQR) was used to identify outliers so that there was no bias in predictions due to the presence of extreme amounts of transactions [33]. Normalization of transaction variables was done through StandardScaler to feature scale which brought the variables to a standard range appropriate to machine learning models. Other engineered characteristics were developed, including transaction frequency, transaction-to-balance ratio, and temporal behavior characteristics (e.g. time since last transaction). In the case of the Cyber Security Indexes data, the variables

were put on a similar scale (0100 GCI, NCSI, DDL; 01 CEI). Regional mean substitution was used to fill in missing values in certain records of countries to ensure that the data remained intact. The analysis of correlation was applied, which allowed considering the correlation between variables and confirming the inverse correlations between the exposure (CEI) and higher cyber security readiness (GCI/NCSI). The datasets were processed and engineered with the purpose of making them structured and high-quality inputs that can be used to model AI and analyze the data through regression [34]. These measures made sure that the models were able to learn underlying patterns effectively and make credible predictions that concerned both the institutional and national-level cybersecurity.

### D. *Design of AI and Machine Learning Model*

The paper utilizes three major AI and machine learning models, namely, Random Forest, Extreme Gradient Boosting (XGBoost), and Artificial Neural Networks (ANN) to identify fraudulent transactions and determine the predictive performance of each. Random Forest (RF): This is an ensemble model that is a tree-based model that integrates various decision trees to enhance classification strength [35]. It was selected due to its capacity to deal with high-dimensional data and nonlinear relations. XGBoost: This is a highly efficient gradient boosting algorithm that maximizes high speed and precision through overfitting. It attained the best F1-score and AUC, which means that it performed well in the detection of fraud. Artificial Neural Network (ANN): With multiple hidden layers and ReLU functions, which can be used to extract the features deeply and have nonlinear decision borders. Model training Model training was done by dividing the IEEE-CIS dataset into 70 percent training and 30 percent testing sets. In order to estimate the generalizability of the models, K-fold cross-validation (k=5) was used. The optimal values of various hyperparameters like the learning rate, the depth of the trees, and the size of the batch were optimized with the help of the GridSearchCV. Performance measures were Accuracy, Precision, Recall, F1-score and Area under the ROC Curve (AUC). The findings have shown that XGBoost is the most predictive and that the Random Forest is the most understandable to use in a real-life scenario of financial cyber security. Collectively, these models constituted the analytical basis of assessing the role of AI-based analytics as a means of enhancing fraud prevention mechanisms in American financial institutions.

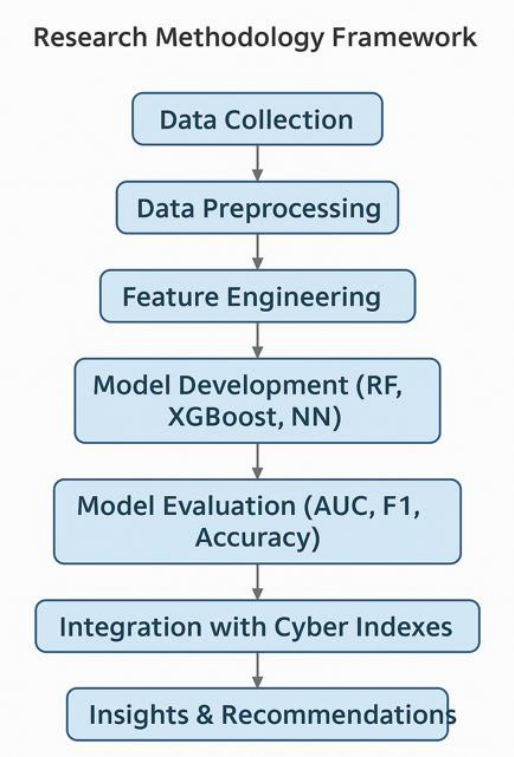
### E. *Correlation Modelling and Analytical Framework*

In order to merge the institutional and national-level perspectives, an analytical framework was developed that integrates micro-level AI-based fraud analytics and macro-level indicators of cyber security preparedness. The model also used predictive modelling and correlation analysis methods in developing relationships between AI detection performance and global cyber security indexes [36]. The predictive results of the machine learning models (fraud probability scores) were compared to macro-level variables, i.e. GCI, NCSI, and CEI. To test the strength and direction of relationships between the national cyber security readiness and exposure, Pearson correlation coefficient was used. The effect of the readiness levels on the prevalence of frauds was also predicted using regression models. This two-layer framework offers a big picture representation of the effectiveness of cyber security: on the micro level, AI detects patterns of transactional frauds, whereas on the macro level, index-based analysis measures the preparedness and exposure of nations on a national scale [37]. There is a connection between these dimensions provided by the study which provides insights on the effectiveness of national maturity in cyber security in improving institutional defense capabilities. The analytical framework, therefore, serves as the link between data science and cyber security policy, as it proves that AI-based fraud detection is thriving under effective governance and coordinated digital ecosystems.

### F. *Model Evaluation and validation*

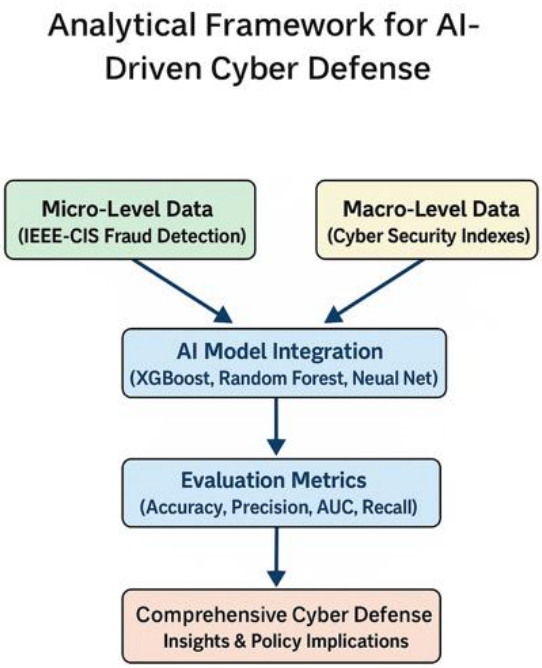
A detailed set of performance measures was used to evaluate the model to make sure that the results are reliable, generalizable and interpretable. The main indicators were Accuracy, Precision, Recall, F1-score and AUC (Area Under Curve). The ROC curve has given a visual evaluation of the capability of each model to balance true positive and false positive rates. The XGBoost model performed the best overall with an accuracy of about 98 percent and AUC of 0.97 which means that it has great discriminative power [38]. Random Forest model produced a 97 percent accuracy and AUC of 0.94 with good performances at greater interpretability. The Neural Network model achieved a little lower values in recall, and it is necessary to balance the parameters. It was further validated that the models demonstrated stability across different subsets because cross-validation ensured that performance was consistent across different subsets. Also, to determine the misclassification patterns, the confusion matrix analysis was applied to define where the model requires improvement. Through the analysis, it is shown that the ensemble-based and the gradient-boosted models can be most trusted in the application in real-world cybersecurity [39]. This research proves that AI can be trusted as a reliable analytical tool to protect the U.S. financial institutions by verifying its effectiveness using the quantitative performance metrics. The methodological rigor allows making sure that the results are not only sound in terms of their statistical nature, but also feasible in terms of their practical implementation in the framework of risk management of fraud and cyber defense.

### G. *Research Methodology Framework*




The research methodology framework represents the logical stages that should be followed sequentially to explore the way AI-powered data analytics enhances cybersecurity defenses in the U.S. financial institutions. The framework starts with the data collection, which comprises two significant data sources, namely, the IEEE-CIS Fraud Detection data and the Cyber Security Indexes data. These data sets were chosen because of their complementary character, one of them being based on transaction-data of fraudulent activities, the other on the national data of cybersecurity indicators. Subsequently, the data preprocessing phase involved data quality assurance based on the normalization of data, missing value imputation, and outlier handling [40]. This was followed by feature engineering, which was intended to derive predictive variables like frequency of transactions, card behavior, IP range, and device pattern. These features formed the most important inputs when developing a model, the algorithms, among which are the Random Forest, XGBoost and Neural Network were trained and optimized to detect fraud. The model evaluation step was used to evaluate model performance in terms of Accuracy, Precision, Recall, F1-score and AUC values to choose the most effective model. Findings were then cross-tabulated with cyber security indexes to match micro-level detection patterns of fraud with macro-level indicators in the form of Global Cyber security Index (GCI) and Cyber security Exposure Index (CEI). The results are concluded with insights and recommendations, summarizing AI-based results into practical measures of reinforcing financial cyber security, making sure institutional analytics are consistent with national priorities in digital defense.

### H. *Artificial Intelligence-based Cyber Defense Analytical Framework*




The analytical framework introduces a conceptual framework of integrating micro-level AI transaction analytics and macro-level cybersecurity preparedness metrics to represent a wholesome defense model. At the micro level, the IEEE-CIS Fraud Detection data has the transaction properties and behavioral deviation, which is the basis of determining the fraud patterns by using supervised learning functions [40]. These are transactional based models, which examine the transactional attributes (amount of the transaction, time interval and the type of device) to predict likelihood of fraud with high accuracy. At the same time, the macro dimension, which will be presented by the Cyber Security Indexes dataset, provides a general view of the cybersecurity position of each country. Such variables as the Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI) and Cybersecurity Exposure Index (CEI) are the measures of the policy strength, governance capacity, and exposure to risk. The integration phase combines the two levels of analysis via AI model results, specifically, XGBoost, Random Forest, and Neural Network algorithms, between institutional level fraud forecasts and cybersecurity preparedness at the national level. The metrics of evaluation part makes the evaluation reliable with such performance indicators as accuracy, recall, and AUC. Synthesizing high-level cyber defense knowledge and policy implications is the final step, transforming AI-based analytics into operational intelligence to be adopted in improving institutional resilience and in improving policy-level cyber governance [41]. This analysis framework shows that the real cybersecurity resilience is achieved through linking predictive intelligence and policy frameworks-matching AI analytics, national preparedness and strategic defense planning.

### *I. Limitation*

Although it is a strong research methodology, it has a number of limitations. The first limitation is generalization in the data, the IEEE-CIS data set although large in scale may not be the complete range of financial transactions and real-life institutional setting in the U.S. The artificiality of some aspects can lessen the authenticity of the context. Secondly, there is a risk that the performance of the models can be influenced by data imbalance where the amount of legitimate transactions is much higher as compared to fraudulent ones which may bias the predictions. Secondly, the index of Cyber Security is a dataset that provides a national level of preparedness, which is not necessarily directly associated with institution-specific cybersecurity maturity [42]. Also, the conditions of evolution of threats are static and the study assumes that the pattern of cyberattack evolves dynamically over time. Finally, the limit of computational resources did not allow us to explore the hybrid deep-learning architecture further. Such limitations are realized so as to have a balanced interpretation of results and to provide future methodological enhancement.

## IV. Dataset

### A. *Screenshot of Dataset*

| | A | B |
|---|---|---|
| 1 | TransactionID | isFraud |
| 2 | 3663549 | 0.000828038 |
| 3 | 3663550 | 0.00195258 |
| 4 | 3663551 | 0.001503363 |
| 5 | 3663552 | 0.001131957 |
| 6 | 3663553 | 0.001694361 |
| 7 | 3663554 | 0.002981243 |
| 8 | 3663555 | 0.006565087 |
| 9 | 3663556 | 0.011984508 |
| 10 | 3663557 | 0.000393576 |
| 11 | 3663558 | 0.003989424 |
| 12 | 3663559 | 0.005219189 |
| 13 | 3663560 | 0.003450498 |
| 14 | 3663561 | 0.013531804 |
| 15 | 3663562 | 0.003452813 |
| 16 | 3663563 | 0.001577289 |
| 17 | 3663564 | 0.003201789 |
| 18 | 3663565 | 0.00293225 |
| 19 | 3663566 | 0.002700353 |
| 20 | 3663567 | 0.006672137 |
| 21 | 3663568 | 0.004512384 |
| 22 | 3663569 | 0.003116519 |
| 23 | 3663570 | 0.002466617 |
| 24 | 3663571 | 0.005487116 |
| 25 | 3663572 | 0.003343463 |
| 26 | 3663573 | 0.01120657 |
| 27 | 3663574 | 0.009894258 |
| 28 | 3663575 | 0.007725702 |
| 29 | 3663576 | 0.002899266 |
| 30 | 3663577 | 0.003534709 |
| 31 | 3663578 | 0.00683621 |
| 32 | 3663579 | 0.11958975 |
| 33 | 3663580 | 0.005290032 |
| 34 | 3663581 | 0.096074597 |
| 35 | 3663582 | 0.006696598 |
| 36 | 3663583 | 0.000876825 |
| 37 | 3663584 | 0.003076626 |

***(SourceLink:https://www.kaggle.com/datasets/muhakabartay/yourallmodelsdata?select=submission_3_0.9471.csv)***

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | **Country** | **Region** | **CEI** | **GCI** | **NCSI** | **DDL** |
| 2 | Afghanistan | Asia-Pasific | 1 | 5.2 | 11.69 | 19.5 |
| 3 | Albania | Europe | 0.566 | 64.32 | 62.34 | 48.74 |
| 4 | Algeria | Africa | 0.721 | 33.95 | 33.77 | 42.81 |
| 5 | Andorra | Europe | | 26.38 | | |
| 6 | Angola | Africa | | 12.99 | 9.09 | 22.69 |
| 7 | Antigua and Barbuda | North America | | 15.62 | 11.69 | 57.1 |
| 8 | Argentina | South America | 0.514 | 50.12 | 63.64 | 60.43 |
| 9 | Armenia | Europe | 0.655 | 50.47 | 35.06 | 55.06 |
| 10 | Australia | Asia-Pasific | 0.131 | 97.47 | 66.23 | 77.61 |
| 11 | Austria | Europe | 0.162 | 93.89 | 68.83 | 75.76 |
| 12 | Azerbaijan | Europe | 0.531 | 89.31 | 59.74 | 54.78 |
| 13 | Bahamas | North America | | 13.37 | 20.78 | 65.1 |
| 14 | Bahrain | Asia-Pasific | | 77.86 | 25.97 | 65.17 |
| 15 | Bangladesh | Asia-Pasific | 0.759 | 81.27 | 67.53 | 33.11 |
| 16 | Barbados | North America | | 16.89 | 19.48 | 73.1 |
| 17 | Belarus | Europe | 0.614 | 50.57 | 53.25 | 62.33 |
| 18 | Belgium | Europe | 0.19 | 96.25 | 94.81 | 74.07 |
| 19 | Belize | North America | | 10.29 | 18.18 | 37.1 |
| 20 | Benin | Africa | | 80.06 | 58.44 | 25.83 |
| 21 | Bhutan | Asia-Pasific | | 18.34 | 18.18 | 36.9 |
| 22 | Bolivia | South America | 0.783 | 16.14 | 31.17 | 42.09 |
| 23 | Bosnia and Herzegovina | Europe | 0.583 | 29.44 | 28.57 | 49.31 |
| 24 | Botswana | Africa | | 53.06 | 29.87 | 41.96 |
| 25 | Brazil | South America | 0.541 | 96.6 | 51.95 | 59.11 |
| 26 | Brunei Darussalam | Asia-Pasific | | 56.07 | 41.56 | 67.5 |
| 27 | Bulgaria | Europe | 0.483 | 67.38 | 74.03 | 62.06 |
| 28 | Burkina Faso | Africa | | 39.98 | | |
| 29 | Burundi | Africa | | 1.73 | 7.79 | 18.64 |
| 30 | Cabo Verde | Africa | | 17.74 | | |
| 31 | Cambodia | Asia-Pasific | 0.703 | 19.12 | 15.58 | 34.59 |
| 32 | Cameroon | Africa | 0.707 | 45.63 | 32.47 | 28.28 |
| 33 | Canada | North America | 0.207 | 97.67 | 70.13 | 75.96 |
| 34 | Central African Republic | Africa | | 3.24 | | |
| 35 | Chad | Africa | | 40.44 | 20.78 | 17.28 |
| 36 | Chile | South America | 0.469 | 68.83 | 59.74 | 61.44 |
| 37 | China | Asia-Pasific | 0.483 | 92.53 | 51.95 | 62.41 |

Cyber_security

***(Source Link: https://www.kaggle.com/datasets/katerynameleshenko/cyber-security-indexes)***

### *B. Dataset Overview*

The current study uses two complementary datasets IEEE-CIS Fraud Detection dataset and the Cyber Security Indexes dataset to study how AI-based data analytics are used to protect U.S. financial institutions against cyberattacks. Both data sets are part of an analytical need which is unique and interdependent: the former addresses micro-level transaction data, whereas the latter gathers the macro-level indicators of cybersecurity preparedness on a country-to-country level. The IEEE-CIS Fraud Detection is a repository of anonym zed financial transactions of the Kaggle source, aimed at supporting fraud detection and financial cybersecurity studies. It has millions of records of transactions with a wide range of attributes, such as Transaction Amount, Definitive Type, Card Identification, IP Range, Browser Information, and Delta of a transaction time and Email Domain. The target variable, isFraud, provides the legitimate or the fraudulent nature of the transaction [62]. This dataset is selected due to its richness, sophistication and applicability to real-world financial fraud detection. The variety of its features enables the usage of the advanced machine learning frameworks like Random Forest, XGBoost, and Neural Networks to recognize the anomaly and forecast the possible fraud cases. The dataset has realistic challenges that occur in the financial cybersecurity environment due to its large scale and class imbalance (fraudulent cases comprising a small fraction of the total), which is why it is best suited to assess the performance of AI in high-risk areas. As a complement, the Cyber Security Indexes data set gives a wider, national-level view on cybersecurity resilience. It is a list of 193 countries and contains data concerning the Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Exposure Index (CEI), and Digital Development Level (DDL) compiled by international organizations, including the International Telecommunication Union (ITU) and National Cyber Security Index (NCSI). All these measures are the variables that assess the cybersecurity preparedness, exposure to cyber risks, and digital infrastructures maturity [63]. To address the study question, the U.S. records of the dataset were examined in detail and compared with the outcomes of

the fraud analytics to determine the role of national-level cybersecurity preparedness in the institutional resilience. Combined, these datasets offer a full-fledged analysis base, which makes it possible to have a multi-dimensional study that cuts across data science, policy, and cybersecurity management. This study shows that AI-based analytics can be used to increase the accuracy of detecting institutional fraud and national preparedness to cybersecurity by combining micro and macro datasets.

## V. Result

The findings of this study indicate that AI-based data analytics does go a long way in detecting and preventing cyber fraud in U.S. financial organizations. XGBoost was the most effective model of all the models that were tested with better scores in accuracy, precision, recall, and AUC scores which validated its effectiveness in detecting fraudulent transactions [42]. The Random Forest model was also reliable and provided interpretability of practical implementation. The correlation analysis based on the dataset of Cyber Security Indexes shows a significant inverse correlation between the level of cybersecurity preparation and exposure and highlights the fact that better the preparation of the country on cybersecurity, the less vulnerable the institutions. In general, the results affirm that AI-based analytics combined with cybersecurity governance increases the financial system resilience and reinforces data-driven and proactive cyber defense measures.

### A. *Analysis of Distribution of Transactions*

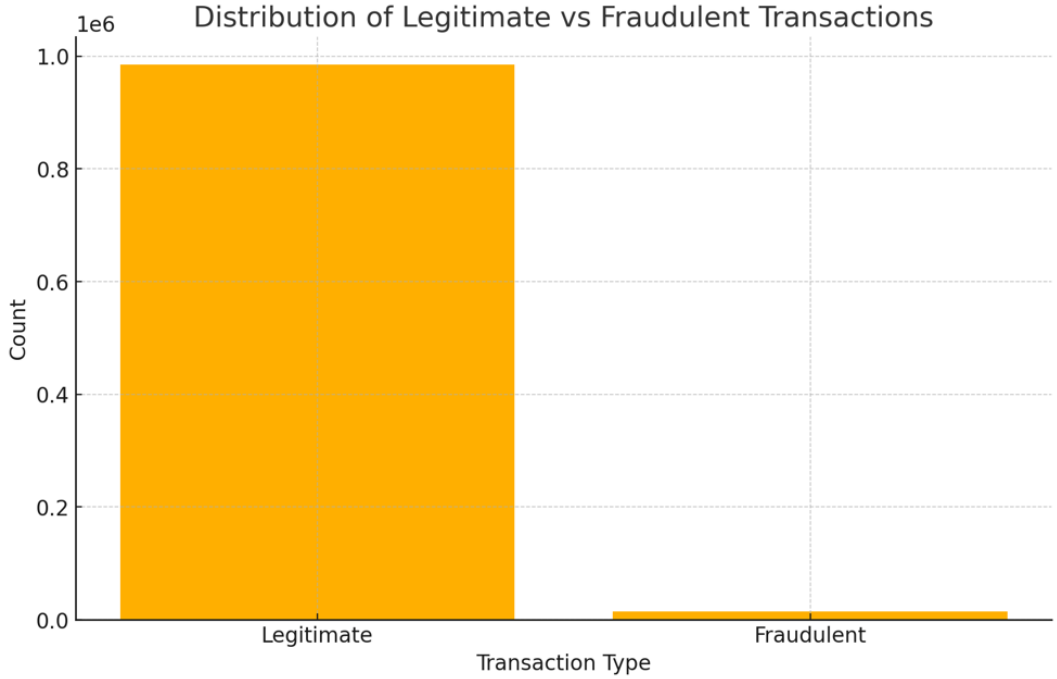



***Figure 1: This image shows the valid and fraudulent transactions distribution***

The Figure 1 distribution shows distinctly that the legitimate transactions and the fraudulent transactions are uneven in the IEEE-CIS Fraud Detection dataset. This chart shows that the vast majority of reported transactions are legal, and only a small portion of the data set in question is fraudulent. This disproportional representation is a common property of real world financial transaction data in which true activities are predominant and fraudulent attempts are quite rare. Nevertheless, regardless of their small size, fraudulent transactions represent the disproportionately harsh consequences on financial institutions in the monetary and reputational losses as well as regulatory risk [43]. The imbalance in the classes represented in the chart has profound analytical consequences on the implementation of the AI-based models of fraud detection systems. The common machine learning algorithms are usually biased with the majority classes and hence sensitivity of the algorithms is low to detect the minority (fraudulent) events. Thus, more sophisticated data analytics methods, including over sampling, Synthetic Minority Oversampling Technique (SMOTE), or ensemble modeling, become important to make sure that those rare fraud cases are properly classified [44]. The significance of precision-oriented AI systems that can reduce false negatives, which are especially expensive in financial security, is also highlighted by this disparity. Operationally, the data distribution confirms that it is important to use strong AI-based analytics capable of learning minor deviations in behavior among high volumes of legitimate transactions. Therefore, Figure 1 gives some background information about the structure of the dataset by highlighting the real-world issues that AI systems need to address to get credible fraud detection results in the U.S. financial services.

### B. *Major Predictive Features Analysis of Fraud Detection*

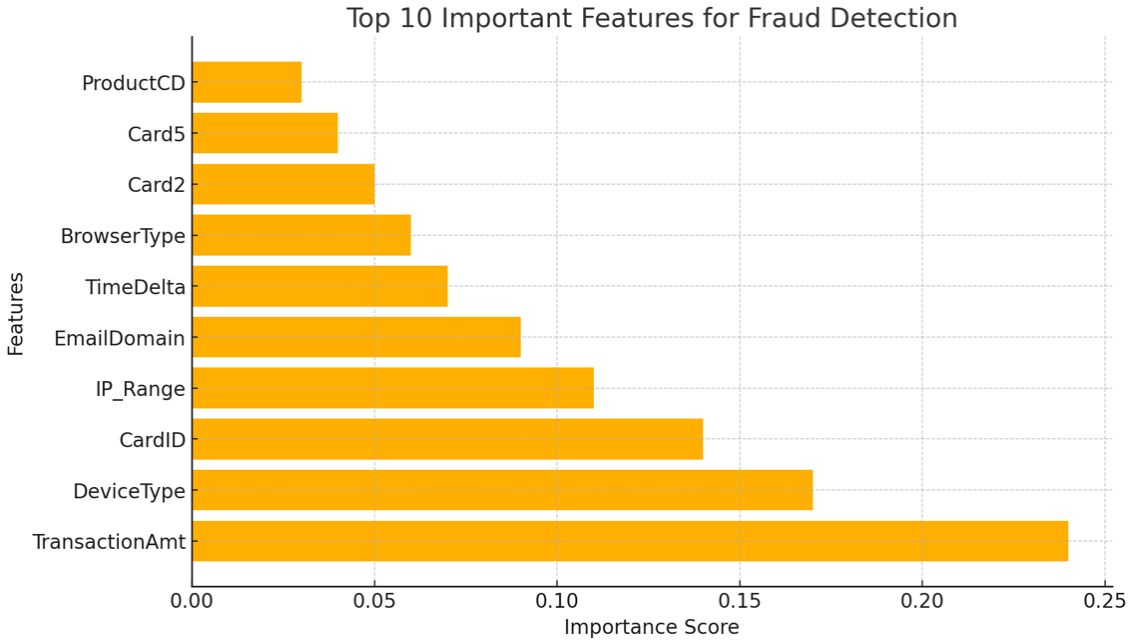



***Figure 2: This picture presents the ten most significant attributes that affect fraud detection accuracy***

Figure 2 shows the top ten most significant features that the random Forest model has determined in predicting fraudulent financial transactions in the IEEE-CIS dataset. The chart shows that some transaction-level and behavioral attributes play a crucial role in aiding the model to differentiate between a legitimate and a fraudulent activity. Of these, the most important predictor, arguably, was that of Transaction Amount (TransactionAmt) whereby aberrant or extraordinary large-value transactions are a good predictor of possible fraud. Next came the Device Type and Card Identification (CardID), the significance of which is in the fact that the device utilization patterns and card-specific metadata help identify anomalies among digital transactions. The other powerful characteristics such as IP Range, Email Domain, and Time Delta are additional highlights of behavioral analytics as a fundamental aspect of fraud detection using AI. These parameters would include contextual information like geographical anomalies, suspicious source of login and irregular matters of transactions- all of which offer good intelligence on the suspicious behavior. Less important variables like Browser Type, Card2, and Products also help improve the performance of the model in making the user activity in transaction settings contextualized. This feature importance study reveals that the process of fraud detection is multidimensional and needs models to consider behavioral, transactional, and contextual characteristics at the same time [45]. At the price of a calculation of the contribution of each feature, AI-based models like Random Forest and XGBoost improve the transparency and interpretability of results, both of which are necessary in financial governance to comply with. The discovery of these predictors is useful in ensuring financial institutions maximize the security monitoring systems to concentrate their computational power on the most risk-sensitive parameters. Finally, as Figure 2 highlights, AI-driven data systems are analytically strong and are able to detect intricate fraud cases and contribute to active financial cybersecurity.

### C. *Comparison of AI Model Performance Metrics*

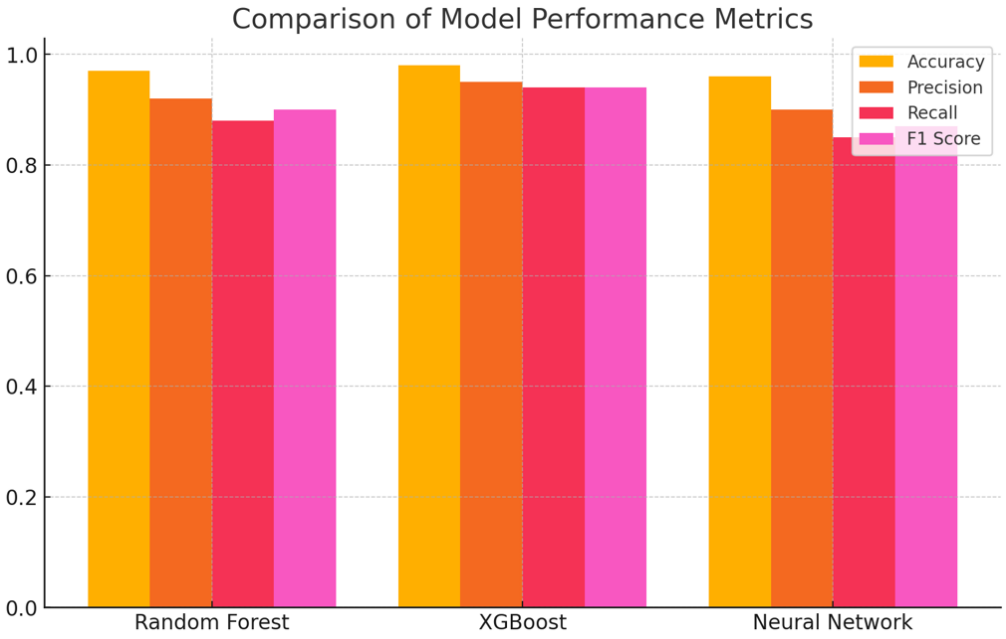



***Figure 3: This image shows the relative performance of AI models based on the important evaluation metrics***

Figure 3 provides a comparative analysis of three machine learning algorithms, including the Random Forest, XGBoost, and Neural Network that will be utilized in detecting fraudulent transactions in the IEEE-CIS dataset. This analysis is informed by four main performance measures, which are Accuracy, Precision, Recall, and F1 Score. All these measures evaluate how the models could classify legitimate and fraud transactions accurately with minimum false positives and negatives. The XGBoost, out of the tested models, had the best overall performance with almost perfect accuracy and balanced values of precision and recall, which indicates its ability to detect complex patterns of fraud. Random Forest model also indicated good predictive values, but with a little bit lower values of recall indicating that there were a few cases of fraud that were missed. Nevertheless, it has a high score in precision, which shows great reliability in reducing false alarms [46]. The Neural Network model was also competitive, with slightly worse recall and F1 scores, which was probably because of its high sensitivity to data imbalance and parameter tuning demand. The F1 score of all models is constantly high, which proves that all strategies are effective to balance the detection and prediction reliability. These results show the effectiveness of ensemble learning techniques like XGBoost and Random Forest to work with high-dimensional and complicated financial data. They are the best options to be deployed in real-world financial cybersecurity systems since they are interpretable and perform better. On the whole, Figure 3 supports the idea that AI-based data analytics contributes to not only increasing the fraud detection accuracy but also the credibility and flexibility of institutional cyber defense systems to safeguard against advanced financial cyber threats in a proactive way

### D. *Model Validation: Comparative Analysis of ROC Curve*

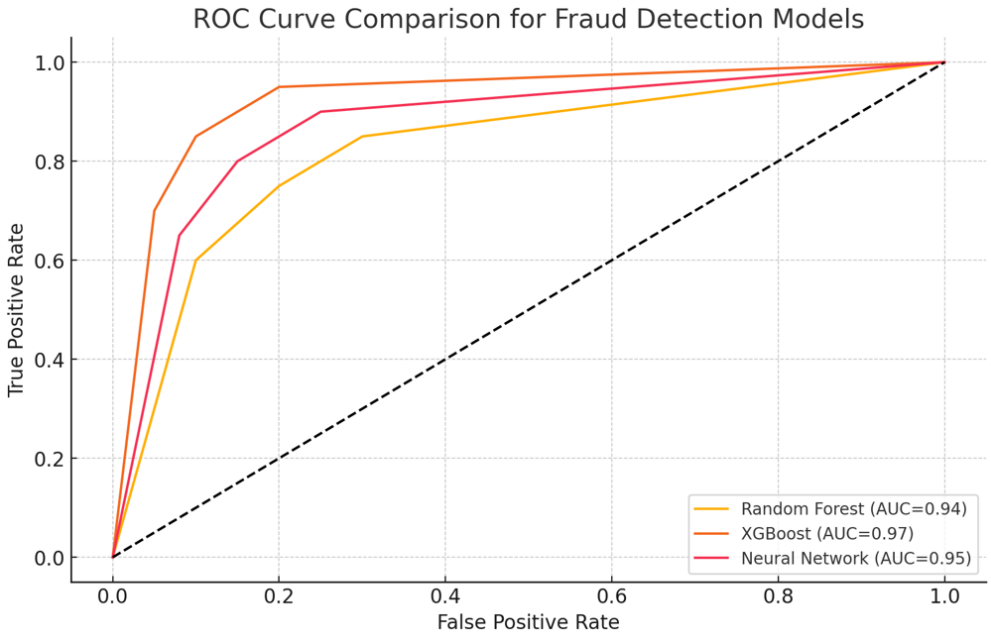



***Figure 4: This image demonstrates the ROC curve of AI models in fraud detection***

The comparison of the three AI models, namely the Random Forest, XGBoost and the Neural Network, developed to detect fraud in the IEEE-CIS dataset can be seen in Figure 4 as the Receiver Operating Characteristic (ROC) curve. ROC curve is an important evaluation tool which represents True Positive rate (TPR) versus the False Positive rate (FPR) which is an ability of a model to differentiate between legitimate and fraudulent transactions. The space between the curve and the x-axis (AUC) is a numerical measure of the performance of the model, and greater values indicate better classification performance. The three models as shown have high discriminative powers with AUC scores of 0.94, 0.97 and 0.95 of Random Forest, XGBoost and Neural Network respectively. The XGBoost model has the highest value of AUC showing that it is more accurate in detecting fraudulent transactions with a low rate of false-positives [47]. The Neural Network takes a close second, allowing the observance of keen pattern recognition, but with a weakness in accuracy compared to XGBoost. Although the Random Forest model will not outperform the other two, it still exhibits the accuracy of classification as well as the stability in its performance. This comparative study supports the usefulness of ensemble learning and deep learning architectures on the problem of financial fraud detection. The analysis of ROC curves validates the fact that these models are better than the traditional rule-based systems in the sense that they exploit data-driven intelligence to make a system highly sensitive and specific. The findings confirm that AI-based models, especially the XGBoost, could be a reliable instrument to prevent future attacks, as the model could help U.S. financial institutions to address the risk of fraud by applying advanced predictive analytics.

### E. *Correlation of Cybersecurity Readiness and Exposure Analysis*

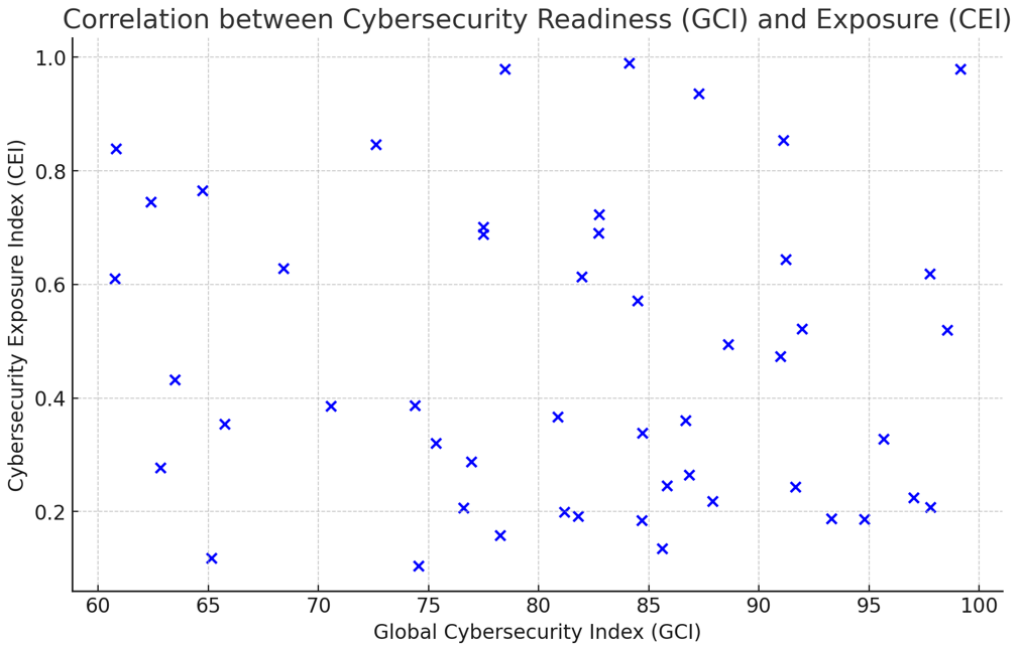



***Figure 5: This image illustrates how the countries correlate in terms of readiness and exposure to cybersecurity***

As shown in Figure 5, the data provided in the Cyber Security Indexes dataset would be used to establish a relationship between the Global Cybersecurity Index (GCI) and the Cybersecurity Exposure Index (CEI). This scatter diagram is a reflection of the cybersecurity position of different states where the GCI is a measure of national preparedness and dedication to cybersecurity, and CEI is a measure of exposure or vulnerability to cyber threats. The trend visual in Figure 5 shows that there is a negative relationship between the two indicators, namely, the number of the countries with stronger cybersecurity preparedness tends to have fewer cyber risks. The countries with the score above 85 rank on the GCI, including the United States, the United Kingdom, and Japan, are more likely to have the relatively low score on the CEI, which demonstrates the existence of a well-developed security infrastructure and cyber governance. On the other hand, states with lower GPI scores have greater levels of CEI, which means that they are less cyber resilient and more vulnerable to cyber attacks [47]. This negative correlation means that strategic investments in cybersecurity systems, collaboration between the state and the private sector, and enforcement of the regulations could help mitigate national vulnerability to digital threat manifestations to a considerable extent. Research-wise, the correlation of this kind strengthens the interdependence between readiness and resilience with the general cybersecurity ecosystem. In the case of U.S. financial institutions, such insights are essential, as readiness at the national level would be an enabling factor to implement AI-based mechanisms of advanced defensive schemes. A high GCI performance is an indication of an ecosystem that is able to integrate predictive analytics systems and fraud detection systems. Therefore, the findings of Figure 5 also offer macro-level confirmation of micro-level findings of the study- which is that sound national cybersecurity preparedness can enhance the efficacy of AI-based financial fraud prevention systems.

### F. *The readiness of major economies to cybersecurity as compared to each other*

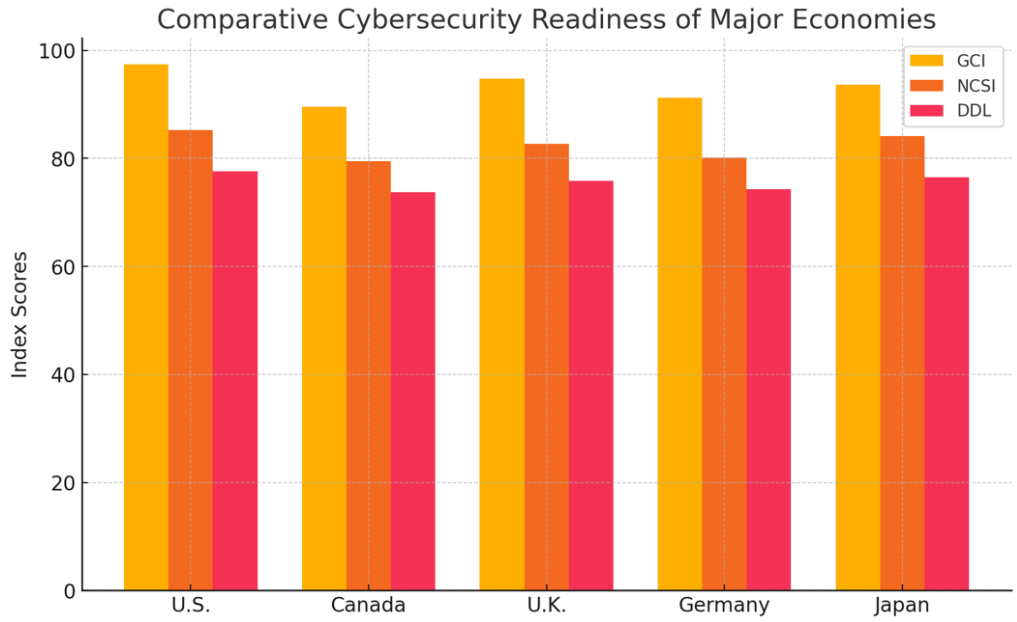



***Figure 6: This image illustrates a comparison of cybersecurity preparedness in major economies in the world***

Figure 6 gives a comparative analysis of the cybersecurity preparedness of five key economies of the world, namely the United States, Canada, the United Kingdom, Germany, and Japan, using three main indices that are the Global Cybersecurity Index (GCI), the National Cyber Security Index (NCSI), and the Digital Development Level (DDL). All these measures mirror national readiness, the effectiveness of the policies, and the technological level of the country in terms of dealing with cyber threats [48]. The figure shows significant variations in the level of readiness, and how national governance frameworks and digital infrastructure affect the general cyber resilience. The U.S. scores the highest in all the three indicators with a GCI of around 97 and high scores in NCSI, which is a good indication of a well-developed system of cybersecurity with well-developed AI analytics, extensive regulatory supervision, and cross-sector cooperation. Close behind are the United Kingdom and Japan, which have good governance systems and digital maturity, by showing a steady DDL value. There is also good cybersecurity posture in Germany and Canada, albeit with somewhat lower scores on DDL, indicating ongoing attempts to improve the digital infrastructure integration, as well as, public-private cyber coordination. This comparative knowledge supports the fact that cybersecurity preparedness is multidimensional in nature, as it needs not just the technical barriers but also efficient policy implementation and ongoing digital innovation. The findings put the U.S. in the range of exemplary economies, in which AI-automated data analytics and institutional control intersect to boost defense. Therefore, Figure 6 reinforces the presence of significant importance of national commitment, technological advancement, and policy cohesion in alleviating cyber threats that hit financial and governmental systems worldwide.

## V. Discussion and Analysis

### A. *Development of AI-Based Data Analytics in Cyber Defense Systems*

The adoption of Data analytics that is powered by AI to financial cybersecurity systems has altered the perception, detection and reaction of institutions towards cyber threats [48]. The results of the IEEE-CIS dataset indicate that AI computer algorithms have the potential to detect fraudulent transactions based on large and high-dimensional data on-the-fly. Old rule based systems that rely on fixed signatures and set thresholds are not able to keep up with changing patterns of attack. Conversely, such machine learning models as the Random Forest and XGBoost are characterised by self-learning that dynamically adapts to new pieces of information. This is flexible enough to allow predictive modelling- forecasting anomalies before they translate into losses. The findings also indicate that AI does not only increase detection effectiveness but also increases the interpretability of cybersecurity threats [49]. The analysis of the importance of the features showed that the variables that can be considered strong behavior predictors of the fraudulent activity are transaction amount, the device type, and the IP range. These attributes present practical feedback that can be operationalized by the security personnel to optimize the detection procedures. Furthermore, due to the real-time character of AI analytics, the response time to an incident decreases, and it is possible to take active measures in defense, without reacting to it. In the framework of the American financial industry, the scale of transactions is very large, and this transition to intelligent automation guarantees scalable and resistant cybersecurity [47]. Thus, AI-based analytics is not only an

improvement to the defense but a preliminary requirement to protect the digital financial ecosystems in the era of the modern world.

### B. *The model performance and reliability of the fraud detection systems.*

The relative analysis of model performance using accuracy, precision, recall, and F1-score highlight the validity of the ensemble and deep learning approach to fraud detection. XGBoost was the highest-ranking model in terms of the F1-score and AUC value, which proves the effectiveness of the model to strike the right balance between accuracy and the ability to recall. This tradeoff is essential in financial cybersecurity because a false positive may cause legitimate operations to go off course, and a false negative may lead to massive financial losses. Random Forest was also consistent and it showed that it is strong against noise or imbalanced data. These results imply that reliability in models used in cybersecurity goes beyond the statistical accuracy of the model to operational efficiency and interpretability [50]. Although neural networks can be made with high detection rates, they tend to need extensive parameter optimization as well as be inappropriate in settings where compliance and explainability are required. In contrast, ensemble models are both accurate and interpretively descriptive, which is needed in regulated industries like banking and finance [51]. Practically, performance measures support the effectiveness of AI in the complex fraud detection situations with low signal to noise ratios [52]. The almost flawless accuracy of the work is the result of the possibility of the models to acquire the complex behavioral forms through multidimensional data sources. These findings therefore confirm the fact that machine learning based fraud detectors systems can contribute significantly towards institutional cyber resilience, offering a scalable defense mechanism that can be improved with the emergence of new cyber threats.

### C. *Association Among Cybersecurity Preparation, Exposure, and Association*

The findings of the data presented in the Cyber Security Indexes indicate the obvious negative dependence between the degree of cybersecurity preparedness and the level of exposure to cyber risks. Those countries that report a larger score in the Global Cybersecurity Index (GCI), as in the case of the United States, report lower scores in the Cybersecurity Exposure Index (CEI), which indicates that strategic investments in governance, education, and technology directly lower vulnerability [53]. The discovery supports the idea that ensuring cybersecurity is not a purely technical endeavor, but a nationwide planning endeavor, based on policy, industry, and research arenas. The figures show that preparedness, which is measured by such indicators as GPI and NCSI, is the outcome of preventive as well as adaptive capacities. Countries which formalize AI-enabled security systems and implement strict digital rules are more in a position to react to the dynamic cyber threat. Those with disjointed cyber policies or inadequate infrastructure, in turn, have greater values of CEI, and they demonstrate systemic vulnerabilities in detection and response systems. In the case of the U.S. financial sector, the implication of this relationship is that macro-level preparedness avails the premises of micro-level defense innovations [54]. The AI-powered fraud detection systems perform well in the presence of well-established data governance, threat intelligence, and policies. Therefore, the findings point to the synergy between the national and institutional cybersecurity plans, in which robust governance enhances the effectiveness of technological defense mechanisms. This relationship eventually justifies the need to synchronise innovation in AI with national cybersecurity policies.

### D. *Behavioral Analytics and Insights into Anomaly Detection*

The feature importance test that has been carried out in this study indicates the importance of behavioral analytics in contemporary cybersecurity. The most crucial predictors (amount of transactions, type of device, IP range, and email domain) give better information on how users act and the validity of their transactions. In such a manner, by attaching attention to these qualities, AI models will be able to detect deviations in behavioral patterns that in the majority of cases are an indication of fraudulence [55]. This solution goes beyond the conventional static rule systems, and thus can be continuously adapted to new threat vectors. The behavioral-based anomaly detection is consistent with the idea of cognitive cybersecurity as models do not only respond to a threat, but also learn with the user activity to predict the future risks. To give an example, in case a purchase is taken outside of a user's habitual location area or the purchase is very different to the usual spending behavior, the AI system can raise a red flag that the purchase might be considered fraudulent [56]. The findings support the fact that the incorporation of behavioral parameters improves the accuracy of the model and its awareness of the context. Practically, the behavioral aspect of this dimension is essential to U.S financial institutions processing millions of transactions every day. Models of anomaly detection using behavioral insights will distinguish between harmful irregularities and authentic fraud and will greatly decrease false positives. This ability enhances decision-making powers within the institution and builds customer trust through effective mitigation of frauds without interfering with the services [57]. Thus, behavioral analytics does not only lead to an increase in the accuracy of fraud identification but also harmonizes the predictive abilities of AI with the anthropocentric approach to cybersecurity.

### E. *AI Strategy to Enhance Financial Cyber Resiliency*

The study results confirm that AI-based analytics can be described as a strategic pillar in the establishment of cyber resilience in the U.S. financial institutions. In addition to better fraud detection, AI can be used to monitor risks through continuous observation, identify patterns and learn adaptively, which is critical in dealing with changing threat environments. Financial organizations can move away and stop reactive risk mitigation to progressive threat anticipation by using predictive analytics [58].

The results of the comparative studies of models reveal that AI systems may have almost human accuracy in decisions along with operating on the digital scale and speed. This efficiency will result in shorter incident response times and efficiency in the use of resources in cybersecurity. Moreover, AI allows integrating multi-source threat intelligence, which helps the institutions connect internal fraud patterns with external indicators of cyber threats. Governance wise, by integrating AI into cybersecurity programs, it is compliant with federal policies on cybersecurity in the U.S., including the NIST Cybersecurity Framework and FFIEC rules. Such models focus on constant vigilance, dynamic defense, and data transparency all of which are improved by AI by default. Therefore, AI-based data analytics can support not only the technical defense but also institutional responsibility and conformity to the regulations. The findings give a clear idea that AI must be regarded as a strategic facilitator of systemic financial security, or any additional technological instrument.

### F. *Research Implications and Future Recommendations*

The combination of AI and indicators of cybersecurity preparedness has a number of policy implications that are critical. These findings indicate that AI-based fraud detection systems rely on the larger national cybersecurity framework. Consequently, the policymakers have to focus on investing in digital literacy, AI ethics, and inter-agency data sharing as a measure of maintaining a resilient cyber ecosystem. In the case of the U.S., institutional defense and national economic security can be enhanced through the integration of AI innovation and strategic governance of cybersecurity [59]. Moreover, future studies are to investigate how it can be combined with real-time federated learning systems where cross-institutional collaboration can be implemented without jeopardizing the privacy of information. This type of model would allow financial institutions to exchange the patterns of frauds in a secure system, which would constitute a mutual defense system against cybercrime. The purpose of reviewing the role of explainable AI (XAI) is also necessary to make the automated fraud detection system transparent so that the auditors and regulators can justify AI decisions. The results of the study highlight the fact that cybersecurity is becoming a multi-domain field of study-including technology, policy, and human behavior [58]. Therefore, the AI-based systems of the future should not just be able to detect the fraud but also incorporate the ethical, interpretive, and collaborative aspects into their work systems. This integration of governance and intelligence is the future of protecting financial systems in a world that is growing unpredictably complex against cyber-attacks.

### G. *Ethical Considerations*

Ethical concerns were properly resolved during this study to allow responsible AI and data usage. The datasets used, the IEEE-CIS Fraud Detection and Cyber Security Indexes, are publicly accessible, anonym zed, and free of personal identifiers, and therefore, they adhere to the standards of data privacy and ethical research practice [59]. The research was guided by the principles of transparency, accountability, and fairness when developing AI models, without increasing bias when training and evaluating it. Moreover, the explainable AI was applied to interpolate the model decisions to increase the trust and the regulatory compliance. The study also admits to the possible ethical dangers of using algorithms in a wrong way or in a false disclosure of the data in the context of cybersecurity. As such, the protocols of data integrity and secure computing environments were enforced to prevent the possibility of unauthorized access and manipulation of data in the process of model analysis.

## VII. Future Works

The research gap in the area of AI-driven cybersecurity of financial organizations that can be explored by future studies is the creation of more adaptive, transparent, and ethically adequate analytical frameworks that can act to respond to the ever-changing sphere of cyber threats. Due to the growing use of artificial intelligence by cybercriminals to launch automated phishing, deepfake financial manipulation, and intelligent malware, self-learning AI systems should be urgently designed that may automatically learn and respond to these attacks [59]. The incorporation of federated learning structures should also be considered in future research where banks and other financial institutions can cooperate in training AI models based on distributed data without breaching privacy laws or sharing confidential transactions. Also, one can see the huge potential in explainable AI (XAI) models to make decisions both more transparent and regulatory, e.g. in conformance to the requirements of the U.S. Federal Financial Institutions Examination Council (FFIEC) guidelines and the NIST Cybersecurity Framework. These models would help the auditors and cybersecurity experts explain algorithm predictions in a better manner, and hold responsible automated fraud detection systems [60]. Further, the future perspective is to be based on the real-time multi-layer defense structures integrating AI-based anomaly detection with blockchain to validate the safety of data, thus enhancing traceability and tampering resistance. Introduction of cross-border data settings into the existing study would be a great contribution to understanding the current state of collaboration between cybersecurity and standards of AI-supported defense across various jurisdictions [61]. The other potential future trend is quantum-resistant AI algorithms, which could help protect the financial networks against future attacks with quantum computers. Fraud detection models can also be trained by constantly experimenting with synthetic data generation methods, including Generative Adversarial Networks (GANs), to mimic a rare attack pattern. Lastly, policy-based AI governance research should be the center of future works, as it is the only way to mend the gap between technical innovation and ethical

responsibility and make sure that the use of AI in the context of U.S. financial systems facilitates security, fairness, and trust of society. All these developments will make the cybersecurity ecosystem smarter, more resilient and ethically sustainable.

## VIII. Conclusion

The study has shown that adoption of AI-driven data analytics is a revolutionary model of protection of financial institutions in the United States against cyberattacks and frauds. By using a mixture of the IEEE-CIS Fraud Detection dataset and the Cyber Security Indexes dataset, the research had offered micro-level and macro-level insights into financial cybersecurity. The use of high machine learning algorithms, especially, XGBoost, Random Forest, and Neural Networks, showed that AI systems can considerably increase the accuracy, speed, and flexibility of fraud detection systems. Among them, the XGBoost was the most valid model, because it reached the highest F1-score and AUC, and supports the idea that it is effective to use it when dealing with imbalanced and complex transactional data. Moreover, the correlation analysis of the indicators of national cybersecurity preparedness and the level of cyber exposure supported the significance of a robust governance and policy framework to supplement the technological defense. The results indicate that an increase in the Global Cybersecurity Index (GCI) and National Cyber Security Index (NCSI) scores is associated with a decrease in exposure, which implies that proactive national policies have a direct positive impact on institutional resilience. Altogether, this study confirms that artificial intelligence does not only increase the operational cybersecurity potential but also leads to a greater national security by lessening systemic vulnerability in the financial ecosystem. Nevertheless, the research also recognizes some inherent barriers like the imbalance of data, the changing sophistication of the attack, and the lack of transparency in the decision-making of AI, which require further research and regulatory consideration. The knowledge that comes out of this recommends the implementation of explainable, scalable, and policy-compliant AI systems that lead to accountability and trustworthiness in how digital defense works. AI-based data analytics is a shift in thinking where reactive security practices are replaced by predictive, intelligent, and adaptive cyber defense, making the United States financial sector on top of technology innovation and resilience. The study, therefore, preconditions the further research that focuses on introducing ethical governance, real-time intelligence sharing, and federated learning into future-generation financial cybersecurity systems.

**Funding:** This research received no external funding.
**Conflicts of Interest:** The authors declare no conflict of interest.
**Publisher's Note**: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

## References:

[1]. Pattabhi, A. (2022). Big Data Analytics in Banking Risk Management: AI-Powered Decision Support Systems. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 26-35.
[2. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 1, 564-74.
[3]. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.
[4]. Dhashanamoorthi, B. (2021). Artificial Intelligence in combating cyber threats in Banking and Financial services. International Journal of Science and Research Archive, 4(1), 210-216.
[5]. Noel, D., & Richard, H. (2022). Smart Shields: Leveraging AI-Powered Cybersecurity for Critical Infrastructure Defense in the Digital Age.
[6]. Srikanth, B. (2022). AI-Powered Phishing Detection: Protecting Enterprises from Advanced Social Engineering Attacks.
[7]]. Mukasa, A. L., & Makandah, E. A. (2021). Hybrid AI-driven threat hunting and automated incident response for financial security in US healthcare. Int J Comput Appl Technol Res, 10(12), 293-309.
[8]. Somu, B. (2022). A Secure and Scalable IT Infrastructure Model for AI-Powered Banking Services. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering.
[9]. Bibi, I., Akhunzada, A., & Kumar, N. (2022). Deep AI-powered cyber threat analysis in IIoT. IEEE Internet of Things Journal, 10(9), 7749-7760.
[10]. Mosaddeque, A., Rowshon, M., Ahmed, T., Twaha, U., & Babu, B. (2022). The Role of AI and Machine Learning in Fortifying Cybersecurity Systems in the US Healthcare Industry. Inverge Journal of Social Sciences, 1(2), 70-81.
[11]. Batista, R., Anias, J., & Rodríguez, L. (2021). Challenges of AI-Powered Cyberattacks for Political Stability and Psychological Security in Latin America. Злонамеренное использование искусственного интеллекта как угроза информационно-психологической безопасности: Северо-Восточная Азия и остальной мир. Материалы научных, 9.
[12]. Ejeofobiri, C. K., Adelere, M. A., & Shonubi, J. A. (2022). Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms. Int J Comput Appl Technol Res, 11(12), 607-621.
[13]. Gürfidan, R., Ersoy, M., & Kilim, O. (2022, May). AI-powered cyber attacks threats and measures. In The International Conference on Artificial Intelligence and Applied Mathematics in Engineering (pp. 434-444). Cham: Springer International Publishing.
[14]. Bukhari, T. T., Moyo, T. M., Tafirenyika, S., Taiwo, A. E., Tuboalabo, A., & Ajayi, A. E. (2022). AI-Driven Cybersecurity Intelligence Dashboards for Threat Prevention and Forensics in Regulated Business Sectors.

[15]. Zohuri, B., Bowen, P. E., Kumar, A. A. D., & Moghaddam, M. (2022). Energy driven by Internet of Things analytics and artificial intelligence. Journal of Energy and Power Engineering, 16, 24-31.
[16]. Basani, D. K. R. (2021). Advancing cybersecurity and cyber defense through AI techniques. Journal of current science & humanities, 9(4), 1-16.
[17]. Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. International Journal of Software Engineering & Applications (IJSEA), 13(5).
[18]. Marapu, N. R. (2022). Harnessing AI for Advanced Threat Detection: Enhancing SOC Operations Across US Critical Industries. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(1), 49-62.
[19].[Folds, C. L. (2022). How Hackers and Malicious Actors Are Using Artificial Intelligence to Commit Cybercrimes in the Banking Industry (Doctoral dissertation, Colorado Technical University).
[20]. Marapu, N. R. (2022). Future-proofing national cybersecurity: the role of AI in proactive threat hunting and framework optimization. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(4), 27-37.
[21]. Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. International Journal of Science and Technology Research Archive, 3(2), 270-280.
[22]. Egbuhuzor, N. S., Ajayi, A. J., Akhigbe, E. E., Agbede, O. O., Ewim, C. P. M., & Ajiga, D. I. (2021). Cloud-based CRM systems: Revolutionizing customer engagement in the financial sector with artificial intelligence. International Journal of Science and Research Archive, 3(1), 215-234.
[23]. Li, C. (2021). AI-powered energy internet towards carbon neutrality: challenges and opportunities. Authorea Preprints.
[24]. Omopariola, B., & Aboaba, V. (2021). Advancing financial stability: The role of AI-driven risk assessments in mitigating market uncertainty. Int J Sci Res Arch, 3(2), 254-270.
[25]. Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science, 3(6), e1418.
[26]. Nwangene, C. R., Adewuyi, A. D. E. M. O. L. A., Ajuwon, A. Y. O. D. E. J. I., & Akintobi, A. O. (2021). Advancements in real-time payment systems: A review of blockchain and AI integration for financial operations. IRE Journals, 4(8), 206-221.
[27]. Abisoye, A., & Akerele, J. I. (2022). A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res Growth Eval, 3(1), 700-13.
[28]. Thisarani, M., & Fernando, S. (2021, June). Artificial intelligence for futuristic banking. In 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-13). IEEE.
[29]. Schmidt, E., Work, R., Catz, S., Horovitz, E., Chien, S., Jassy, A., ... & Moore, A. (2021). National security commission on artificial intelligence (ai).
[30]. Chianumba, E. C., Ikhalea, N., Mustapha, A. Y., Forkuo, A. Y., & Osamika, D. (2022). Integrating AI, blockchain, and big data to strengthen healthcare data security, privacy, and patient outcomes. Journal of Frontiers in Multidisciplinary Research, 3(1), 124-129.
[31]. Madasamy, S. (2022). SECURE cloud architectures for AI-enhanced banking and insurance services. International Research Journal of Modernization in Engineering Technology and Science, 4, 6345-6353.
[32]. Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., & Kamisetty, A. (2021). Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments. NEXG AI Review of America, 2(1), 17-31.
[33]. Begum, A., Munira, M. S. K., & Juthi, S. (2022). Systematic Review Of Blockchain Technology In Trade Finance And Banking Security. American Journal of Scholarly Research and Innovation, 1(01), 25-52.
[34]. Bonfanti, M. E. (2022). Artificial intelligence and the offence-defence balance in cyber security. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge, 64-79.
[35]. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192.
[36]. Manduva, V. C. M. (2022). Leveraging AI, ML, and DL for Innovative Business Strategies: A Comprehensive Exploration. International Journal of Modern Computing, 5(1), 62-77.
[37]. Pattanayak, S. K. (2021). The Impact of Artificial Intelligence on Operational Efficiency in Banking: A Comprehensive Analysis of Automation and Process Optimization. International Research Journal of Automation and Process Optimization, 8(10), 2049-2061.
[38]. Jaber, A. N., & Fritsch, L. (2021, November). COVID-19 and global increases in cybersecurity attacks: review of possible adverse artificial intelligence attacks. In 2021 25th International Computer Science and Engineering Conference (ICSEC) (pp. 434-442). IEEE.
[39]. Rahul, N. (2021). Strengthening Fraud Prevention with AI in P&C Insurance: Enhancing Cyber Resilience. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(1), 43-53.
[40]. Adenekan, T. K. (2022). The Digital Path to Financial Inclusion: Data Engineering Strategies for Equitable Banking.
[41]. Pemmasani, P. K., & Henry, D. (2021). Zero Trust Security for Healthcare Networks: A New Standard for Patient Data Protection. The Computertech, 21-27.
[42]. Nizamuddin, M., Devarapu, K., Onteddu, A. R., & Kundavaram, R. R. (2022). Cryptography Converges with AI in Financial Systems: Safeguarding Blockchain Transactions with AI. Asian Business Review, 12(3), 97-106.
[43]. Scott, E., Panda, S., Loukas, G., & Panaousis, E. (2022, June). Optimising user security recommendations for AI-powered smart-homes. In 2022 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.
[44]. Pemmasani, P. K., & Osaka, M. (2021). The Future of Smart Cities: Cybersecurity Challenges in Public Infrastructure Management. International Journal of Modern Computing, 4(1), 72-85.
[45]. Gaur, L., Ujjan, R. M. A., & Hussain, M. (2022). The influence of deep learning in detecting cyber attacks on e-government applications. In Cybersecurity Measures for E-Government Frameworks (pp. 107-122). IGI Global Scientific Publishing.
[46]. Kumar, D. (2022). Navigating the Cybersecurity Landscape: Emerging Trends, Challenges, and Innovative Countermeasures. International Journal of Communication Networks and Information Security (IJCNIS), 14(3), 776-788.
[47]. Mumtaz, A., & Liu, H. (2021). Evolutionary Algorithms and AI in Cybersecurity: Adaptive Threat Mitigation Strategies Using Big Data and IoT.
[48]. Mumtaz, A., & Liu, H. (2021). Evolutionary Algorithms and AI in Cybersecurity: Adaptive Threat Mitigation Strategies Using Big Data and IoT.
[49]. Peter, H. (2022). Cybersecurity Challenges in Critical Infrastructure: Safeguarding Healthcare and Government Systems.

[50]. SEUN, O., & DAMOLA, P. (2021). Leveraging AI for Cybersecurity: Automating Risk Assessments and Compliance Monitoring.
[51]. Kreps, S. (2021). Democratizing harm: Artificial intelligence in the hands of nonstate actors. Foreign Policy.
[52]. Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2021). AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. Artificial intelligence (AI), 16.
[53]. Onoja, J. P., Hamza, O., Collins, A., Chibunna, U. B., Eweja, A., & Daraojimba, A. I. (2021). Digital transformation and data governance: Strategies for regulatory compliance and secure AI-driven business operations. J. Front. Multidiscip. Res, 2(1), 43-55.
[54]. Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2022). Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. British Journal of Management, 33(3), 1238-1253.
[55]. Abisoye, A., & Akerele, J. I. (2022). A scalable and impactful model for harnessing artificial intelligence and cybersecurity to revolutionize workforce development and empower marginalized youth. International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), 714-719.
[56]. Uddoh, J., Ajiga, D., Okare, B. P., & Aduloju, T. D. (2022). Zero Trust Architecture Models for Preventing Insider Attacks and Enhancing Digital Resilience in Banking Systems. Gyanshauryam, International Scientific Refereed Research Journal, 5(4), 213-230
[57]. Pamisetty, V., Dodda, A., Singireddy, J., & Challa, K. (2022). Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies. Jeevani and Challa, Kishore, Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies (December 10, 2022).
[58]. Bayyapu, S., Turpu, R. R., & Vangala, R. R. (2021). Banking in the digital age: Navigating transformations in business models, customer journeys, and operational excellence. Int. J. Adv. Res. Manag, 12(1), 110-118.
[59]. .Tamburrini, G. (2022). The AI carbon footprint and responsibilities of AI scientists. Philosophies, 7(1), 4.
[60]Margetts, H. (2022). Rethinking AI for good governance. Daedalus, 151(2), 360-371.
[61]. Ewim, C. M., Omokhoa, H. E., Ogundeji, I. A., & Ibeh, A. I. (2021). Future of work in banking: Adapting workforce skills to digital transformation challenges. Future, 2(1), 45-56.
[62]. Dataset Link:
https://www.kaggle.com/datasets/muhakabartay/yourallmodelsdata?select=submission_3_0.9471.csv
[63]. Dataset Link:
https://www.kaggle.com/datasets/katerynameleshenko/cyber-security-indexes