World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity

Oladipupo Dopamu [1,*], Joseph Adesiyan [2] and Femi Oke [1]

[1] *Department of Computer Sciences, Western Illinois University, Macomb Illinois USA.*
[2] *Department of Applied Statistics and Decision Analytics, Western Illinois University, Macomb Illinois USA.*

World Journal of Advanced Research and Reviews, 2024, 21(03), 964–979

Publication history: Received on 28 January 2024; revised on 07 March 2024; accepted on 09 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0791

Abstract

As cyber threats and regulations become increasingly complex, financial institutions in the U.S. are in need of innovative cyber security solutions. This study examines the potential for artificial intelligence (AI) in addressing this problem. Artificial intelligence has significant potential for real-time threat detection, automated compliance processes, and proactive risk management. Nonetheless, ethical considerations, concerns about personal data privacy, and potential biases in AI algorithms require careful consideration. In light of this, the research proposes recommendations for developing innovative AI solutions. In addition, it addresses ethical and privacy concerns, as well as providing policy recommendations for the responsible and effective adoption of AI in the financial sector. This research highlights AI's potential to significantly enhance security and risk management for financial institutions. Additionally, it emphasizes responsible and ethical implementation.

Keywords: Data privacy; AI-Assisted compliance; Cybersecurity; Risk management; Financial institutions; Ethical considerations; Innovative AI solutions.

1. Introduction

1.1. Background and Significance: Growing Cybersecurity Challenges, Regulatory Complexity, and Artificial Intelligent Potential

As cyber threats and regulations become increasingly complex, financial institutions in the U.S. are in need of innovative cyber security solutions. This study examines the potential for artificial intelligence (AI) in addressing this problem. Artificial intelligence has significant potential for real-time threat detection, automated compliance processes, and proactive risk management. Nonetheless, ethical considerations, concerns about personal data privacy, and potential biases in AI algorithms require careful consideration. In light of this, the research proposes recommendations for developing innovative AI solutions. In addition, it addresses ethical and privacy concerns, as well as providing policy recommendations for the responsible and effective adoption of AI in the financial sector.

This research highlights AI's potential to significantly enhance security, risk management, and compliance for financial institutions. Additionally, this research emphasizes responsible and ethical implementation. Increasing challenges and complexities are accompanying the cybersecurity landscape's rapid evolution. This emergence is driven by various factors, including the infinite volume of data generated. Furthermore, digital devices and cyber threats drive this trend. Regulatory environments around the world are becoming increasingly complicated as governments attempt to protect consumers, ensure data privacy, and safeguard national security. Despite these challenges and complexities, Artificial

* Corresponding author: Oladipupo Dopamu

Intelligence (AI) has emerged as an essential tool with the potential to transform cybersecurity practices, regulatory compliance, and threat mitigation strategies.

The finance services industry is increasingly dependent on technology, which exposes it to a growing range of cyber threats. The financial sector is constantly under pressure to protect its systems and data from sophisticated malware attacks and social engineering scams. In light of this, cybersecurity regulations have been issued by both government agencies and industry officials in response to these concerns. These regulations are in an effort to safeguard sensitive personal and business information and protect consumers. However, financial institutions face substantial challenges in keeping pace with the evolving threat landscape while adhering to a variety of frequently updated regulations.

AI-enabled solutions are capable of analyzing vast amounts of data, detecting, and responding to threats in real time, and adapting to evolving attack methods as they emerge. Financial institutions may be able to streamline their compliance efforts through the use of artificial intelligence, enhance their cybersecurity posture, and ultimately mitigate the risks associated with data breaches.

While promising, each solution comes with its own considerations. AI/ML requires robust data infrastructure and expertise for effective implementation. Blockchain solutions are still evolving, and their integration with existing systems needs careful assessment. Zero - trust adoption necessitates significant changes in security architecture and processes. Collaborative threat intelligence requires building trust and overcoming potential data privacy concerns. Evaluating the feasibility of each solution based on individual institutional resources and capabilities is crucial. Additionally, assessing the potential impact of each solution on factors like security effectiveness, operational efficiency, and cost – effectiveness is vital for informed decision – making (Oladipupo M. Dopamu, 2024).

1.2. Rising cyber threats pose significant risks to financial institutions and consumer data.

The study examines the process of escalating cybersecurity threats targeting the financial sector. It further reviews and analyzes the increasing sophistication and volume of cyberattacks such as ransomware, phishing, and advanced persistent threats (APTs). This, coupled with the expanding attack surface due to IoT, cloud adoption, and remote work, creates a critical risk for financial institutions and consumer data they manage.

Due to the interconnectedness of the US financial system, individual vulnerabilities may become sector-wide concerns. In light of the gravity of the situation, financial institutions are actively ramping up their cybersecurity defenses. As threats become more complex, they are increasingly turning to advanced technologies like artificial intelligence (AI) for better detection and response. Additionally, regulatory bodies are stepping up their efforts by enforcing stricter cybersecurity regulations to ensure robust protection for both institutions and consumer data.

The study reveals the urgent need for a multifaceted approach to protect consumer privacy and the U.S. financial system. This includes a dynamic, technology-driven cybersecurity strategy by financial institutions, coupled with strict adherence to regulatory standards. It is only through this combined effort that we can mitigate cyber threats and ensure the integrity and stability of the financial sector.

1.3. Complex and Evolving Regulatory Landscape Further Complicates Cybersecurity Efforts.

The regulatory landscape governing cybersecurity and data protection is increasingly becoming complex and fragmented, significantly impacting organizations worldwide. This complexity arises from stringent requirements imposed by a variety of laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and other similar regulations across different jurisdictions. These legal frameworks are crafted to bolster data security and privacy, yet they introduce a layered complexity of compliance for entities operating internationally, where non-compliance risks substantial financial penalties, reputational harm, and loss of consumer trust.

Particularly for U.S. financial institutions, this evolving regulatory environment poses a multifaceted challenge to sustaining effective cybersecurity measures. Institutions must navigate through a dense thicket of federal and state laws, including the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and various state-level directives, all of which contribute to a hefty compliance burden. This situation is further complicated by the dynamic nature of cyber threats and the continuous evolution of regulatory standards, necessitating a perpetual state of agility.

Moreover, financial institutions are tasked with managing the nuanced demands of data protection and privacy, alongside the imperative to integrate new technologies within the confines of existing regulatory frameworks. The

adoption of innovations such as cloud computing, artificial intelligence, and blockchain technologies, while promising enhanced operational efficiency and service delivery, must be carefully balanced against compliance obligations.

To effectively address these challenges, a sophisticated approach is essential. This includes the integration of cybersecurity initiatives with regulatory compliance efforts, the provision of regular training for staff on the latest cyber threats and compliance requirements, the adoption of technology solutions to automate and streamline compliance processes, and proactive engagement with regulatory bodies. Such strategies enable financial institutions to adeptly navigate the regulatory maze, ensuring not only adherence to compliance mandates but also the safeguarding of sensitive information against cyber threats, thereby maintaining the integrity and trust of the financial system.

1.4. AI Presents a Promising Avenue for Enhanced Threat Detection, Compliance Automation, and Risk Management.

In the rapidly evolving digital landscape, U.S. financial institutions face mounting cybersecurity threats and a complex regulatory framework. Artificial Intelligence (AI) emerges as a transformative solution, offering a pathway to significantly enhance cybersecurity measures, streamline compliance processes, and bolster risk management strategies. AI's ability to analyze vast datasets in real-time enables unprecedented threat detection capabilities, swiftly identifying potential cyber-attacks before they can inflict harm. This proactive stance on cybersecurity is essential in protecting the sensitive financial and personal information entrusted to these institutions.

Moreover, the regulatory responsibilities imposed on financial institutions are both stringent and multifaceted, comprising laws like the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act. AI can automate the tedious and error-prone tasks of monitoring and reporting, ensuring compliance with these regulations efficiently and effectively. This automation not only reduces the risk of human error but also frees up valuable resources that can be redirected towards strategic initiatives.

Risk management, a critical concern for financial institutions, also benefits from AI's predictive analytics capabilities. By forecasting potential risks with greater accuracy, institutions can preemptively address vulnerabilities, making strategic decisions that safeguard their operations and their clients' interests. However, the integration of AI into financial services must be approached with caution. Ethical considerations, the potential for algorithmic bias, and the imperative to protect customer data privacy are challenges that must be meticulously managed. Ensuring that AI systems are transparent, fair, and compliant with regulatory standards is paramount.

1.5. Research Objectives - Proposing Innovative Solutions, Addressing Ethical Concerns, and Offering Policy Implications

This research aims to explore the potential of AI-assisted regulatory compliance for cybersecurity within US financial institutions. The key objectives are:

Identify and propose innovative solutions for integrating AI into cybersecurity compliance processes. This includes exploring how AI can automate threat detection, streamline regulatory reporting, and optimize risk management.

Address ethical and data privacy concerns associated with AI-powered compliance solutions. The paper will examine potential biases in AI algorithms, the need for explainability and transparency in AI decisions, and data security considerations.

Develop policy recommendations for regulators and financial institutions to facilitate the responsible and effective use of AI for cybersecurity compliance. This includes exploring regulatory frameworks, best practices, and collaboration strategies between stakeholders.

1.5.1. Key Points

- Identify innovative AI solutions for enhancing cybersecurity compliance.
- Address ethical and data privacy concerns inherent in AI-powered systems.
- Develop policy recommendations for responsible and effective AI adoption.

1.6. Scope and Limitations: Specific Focus on US Financial Institutions and Relevant Regulations

This research focuses specifically on the application of AI-assisted regulatory compliance for cybersecurity within US financial institutions. While acknowledging the global trends and advancements in AI for cybersecurity, the specific regulatory landscape and compliance requirements of other countries will not be comprehensively addressed.

Additionally, the research will primarily consider regulations issued by federal agencies such as the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Securities and Exchange Commission (SEC). Industry-specific regulations and self-regulatory organization (SRO) guidelines may be addressed based on their relevance to the chosen focus area.

1.6.1. Key Points

Research scope is limited to US financial institutions and relevant regulations.

Focus on federal agency regulations primarily, with potential consideration of industry-specific guidelines.

2. Review of Related Studies

2.1. Cybersecurity Regulations in US Financial Services: Key Regulations, Challenges, and Trends

2.1.1. Introduction

Navigating the cybersecurity landscape for US financial institutions requires understanding the intricate web of regulations. This section analyzes current key regulations, challenges, and recent trends shaping the regulatory environment.

2.1.2. Current Key Regulations

Securing Rights: *Legal Frameworks for Privacy and Data Protection in the Digital Era (J Babikian, 2023)*

The proliferation of digital technologies, including social media, cloud computing, and Internet of Things (IoT) devices, has transformed the way individuals interact, communicate, and conduct transactions. While these advancements offer numerous benefits, they also raise significant concerns regarding the collection, storage, and use of personal data. Against this backdrop, the importance of robust legal frameworks to safeguard privacy rights and ensure data security cannot be overstated (J. Babikian, 2023).

Federal Information Security Management Act (FISMA): *Applies to institutions holding government data (Board of Governors of the Federal Reserve System, 2023)*

Based on FISMA (2023) reviews, agencies and institutions must continually monitor FISMA accredited systems to identify potential weaknesses. Any changes should be documented in the System Security and Privacy Plan (SSPP). Continuous monitoring will also allow agencies to respond quickly to security incidents or data breaches. CMS is working towards a more robust approach for continuous monitoring through programs like Continuous Diagnostics and Mitigation and Ongoing Authorization.

Bank Secrecy Act (BSA)/Anti-Money Laundering (AML): *Combats financial crime and mandates cybersecurity measures (Financial Crimes Enforcement Network, 2023)*

Criminals have long used money-laundering schemes to conceal or "clean" the source of fraudulently obtained or stolen funds. Money laundering poses significant risks to the safety and soundness of the U.S. financial industry. With the advent of terrorists who employ money-laundering techniques to fund their operations, the risk expands to encompass the safety and security of the nation. Through sound operations, banks play an important role in helping investigative and regulatory agencies identify money-laundering entities and take appropriate action (Cybersecurity and Financial System Resilience Report, 2023).

Securities and Exchange Commission (SEC) Regulation S-P: *Protects investor data and requires cybersecurity policies (Board of Governors of the Federal Reserve System, 2023)*

The Commission's proposal would require broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") to adopt written policies and procedures for an incident response program to address unauthorized access to or use of customer information. The proposed amendments would also require, with certain limited exceptions, covered institutions to provide notice to individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. The proposal would require a covered institution to provide this notice as soon as practicable, but not later than 30 days after the covered

institution becomes aware that an incident involving unauthorized access to, or use of customer information has occurred or is reasonably likely to have occurred *(Board of Governors of the Federal Reserve System, 2023).*

The proposed amendments would also make a number of additional changes to Regulation S-P, including:

Broadening and aligning the scope of the safeguards rule and disposal rule to cover "customer information," a new defined term. This change would extend the protections of the safeguards and disposal rules to both nonpublic personal information that a covered institution collects about its own customers and to nonpublic personal information that a covered institution receives about customers of other financial institutions (SEC, 2023).

Extending the safeguards rule, including the proposed enhancements, to transfer agents registered with the Commission or another appropriate regulatory agency, and expanding the existing scope of the disposal rule to include transfer agents registered with another appropriate regulatory agency rather than only those registered with the Commission; and

Conforming Regulation S-P's existing provisions relating to the delivery of an annual privacy notice for consistency with a statutory exception created by Congress in 2015 *(Board of Governors of the Federal Reserve System, 2023).*

New York Department of Financial Services (NYDFS) Cybersecurity Regulation: *Stringent cybersecurity requirements for institutions operating in New York (New York State Department of Financial Services, 2023).*

On November 1, 2023, New York Department of Financial Services (NYDFS or the "Department") released the finalized revisions (the "Second Amendment") to 23 NYCRR Part 500 (Part 500) – the most significant modifications to Part 500 since it was first enacted in 2017 and established cybersecurity requirements for NYDFS-regulated entities. The revisions, the Department explains in the introduction to its Cybersecurity Resource Center, are aimed at addressing the changes in the increasing sophistication of threat actors, the prevalence of and relative ease in executing cyberattacks, and the availability of additional controls to manage cyber risk (at a reasonable cost). These changes mark the culmination of an approximately yearlong effort, which first began in July 2022, when the Department published a "pre-proposed" draft amendment, which was revised first on November 9, 2022, and again on June 28, 2023, before being finalized on November 1, 2023. Throughout this process, the NYDFS solicited, considered, and responded to public comments (NYDFS Finalize Amendments to Cybersecurity Regulation, 2023).

2.2. Regulation Challenges

2.2.1. Regulatory overlap: The review (Lachlan, R., et al., 2022).

Regulatory failure can result from any number of causes. Failure is generally identified when regulation does not achieve its purpose, or when the costs of regulation are greater than its benefits (Aldridge, 2022; Wolf, 1979). Poor designs, unpopular rules, and power imbalances between regulated entities and regulators can impose costs and externalities that outweigh any gains achieved. Regulatory failure caused by overlapping regulations is ubiquitous, with examples in all jurisdictions across a range of disciplines. Identifying that regulatory overlap can lead to failure means it has been identified as problematic. Indeed, some literature suggests that overlap can obscure policy objectives and hinder the development of effective and clear regulation. In addition, observations indicate that regulatory overlap can inflict real costs on businesses through repetitive inspections and data collection efforts (Lachlan, R., et al., 2022).

2.2.2. Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure (GAO, 2023)

According to Government Accountability Office (GAO) 2023 report: In September 2022, we reported that CISA, FBI, and Secret Service provide assistance in preventing and responding to ransomware attacks on tribal, state, local, and territorial government organizations. The agencies coordinated through existing mechanisms—such as interagency detailees and field-level staff—and demonstrated coordination on a joint ransomware website, guidance, and alerts. However, respondents identified challenges related to awareness, outreach, and communication. Further, the three agencies had not addressed aspects of six of seven key practices for interagency collaboration in their ransomware assistance to tribal, state, local, and territorial governments. For instance, existing interagency collaboration on ransomware assistance to tribal, state, local, and territorial governments was informal and lacked detailed procedures (GAO, 2023).

2.2.3. Resource Constraints: An Executive View of Key Cybersecurity Trends and Challenges in 2023 (Andy Lim, 2023).

The threat landscape continues to expand with the increasing connectivity of devices and systems through the Internet of Things (IoT) and the proliferation of digital technologies. Cyberattacks such as ransomware, phishing and insider threats remain pervasive and pose significant risk to enterprises, governments, and individuals alike. Although these threats are nothing new, as data continue to be produced and stored in greater volumes, and as connectivity expands globally, the attack surface has become more exploitable with gaps and vulnerabilities that are appealing to criminal and nation-state hackers (Brooks, C., 2023). In 2023, cyberthreats are expected to rise as unrest around the world contributes to an increase in cybercrimes (Kaspersky, 2022). Malware attacks (e.g., ransomware attacks) are also expected to target more enterprises (Cook S., 2024).

2.2.4. Technology Trends: An Executive View of Key Cybersecurity Trends and Challenges in 2023 (Andy Lim, 2023).

Based on Andy Lim (2023), emerging technologies such as quantum computing, 5G networks and edge computing are being adopted at a rapidly increasing rate. However, this is introducing new cybersecurity challenges across several areas:

2.2.5. Quantum computing

Encryption vulnerabilities—Quantum computers have the potential to break commonly used encryption algorithms, such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), that currently provide secure communication and data protection. This raises concerns about the privacy and integrity of sensitive data, including financial transactions and personal information (Andy Lim, 2023).

Post-quantum cryptography—The need to develop and implement post-quantum cryptographic algorithms that are resistant to quantum attacks is a challenge. Ensuring a smooth transition from traditional encryption to post-quantum cryptography is crucial to maintain secure communication in the quantum computing era (Andy Lim, 2023).

2.2.6. 5G networks

Increased attack surface—The widespread deployment of 5G networks significantly expands the attack surface, as there are more connected devices and a higher volume of data transmission. This poses challenges in terms of securing a larger and more complex ecosystem, including IoT devices, autonomous vehicles, and critical infrastructure (Andy Lim, 2023).

Network slicing and virtualization—The dynamic nature of 5G networks, which includes features such as network slicing and virtualization, introduces new vulnerabilities and potential points of exploitation. Proper segmentation and isolation between network slices and virtualized network functions are critical to prevent unauthorized access and data breaches (Andy Lim, 2023).

2.2.7. Edge computing

Distributed security—For edge computing, data processing and storage occur closer to the source of data generation. This distributed architecture creates challenges in ensuring consistent security measures across a decentralized infrastructure, making it essential to secure edge devices, gateways, and communication channels effectively (Andy Lim, 2023).

Latency and bandwidth constraints—Edge computing emphasizes low-latency and real-time processing, which may limit the resources available for robust security measures. Balancing security requirements with the constraints of latency and bandwidth is crucial to prevent vulnerabilities and ensure data integrity (Andy Lim, 2023).

These technologies bring opportunities for innovation and efficiency, but also raise concerns about their potential impact on security, privacy, and data integrity. It is essential to prioritize research and development in secure quantum-resistant cryptography, network segmentation, threat detection and secure architecture design to mitigate risk and address the evolving cybersecurity landscape introduced by these technologies (Andy Lim, 2023).

2.3. Existing Trends

2.3.1. Risk-Based Approach: OECD Regulatory Policy Outlook 2021 (OECD, 2021).

Risk-focus and risk-proportionality have been increasingly used by governments and regulators when designing and delivering regulation. Risk helps improve the effectiveness and efficiency of regulation. It is crucial in the perspective of

achieving public outcomes at every step of the regulatory policy cycle, while minimizing burden and unintended side effects of regulation and rules. The use of risk is however unequally spread across countries and regulatory area. Also, many impediments to its utilization exist, ranging from resistance in institutions to the over-estimation of the effectiveness of "non-risk-based" regulation. The COVID-19 crisis has shown the obstacles that regulation can pose to response needs when it is not in line with a risk-based approach, nor flexible enough (OECD, 2021).

Collaboration and Information Sharing: *Partnerships between the public and private sectors that foster Information Sharing (Cybersecurity & Infrastructure Security Agency, 2023).*

As the national coordinator for critical infrastructure security and resilience, CISA has developed and implemented numerous information sharing programs to promote resources and tools that help our partners build security and resilience. These programs include awareness and outreach campaigns like the annual Cybersecurity Awareness Month (CAM) and broader national awareness programs that offer partner toolkits. Through these programs, CISA develops and shares substantive information with the private sector and with state, local, tribal, and territorial governments. Recognizing cybersecurity threat actors are not constrained by geographic boundaries, CISA fosters relationships with international partners to promote collaborative information sharing, cybersecurity best practices, and partnership models across the globe (Cybersecurity & Infrastructure Security Agency, 2023).

Focus on Third-Party Risk Management: *Interagency Guidance on Third-Party Relationships (Board of Governors of the Federal Reserve System, 2023).*

On July 19, 2021, the agencies published for comment proposed guidance for banking organizations on managing risks associated with third-party relationships (proposed guidance) (86 Federal Register 38182, 2021). The proposed guidance laid out a risk management framework covering various stages in the life cycle of third-party relationships, including planning, due diligence, contract negotiation, ongoing monitoring, and termination, and provided examples of risk management considerations at each stage. The agencies invited comment on all aspects of the proposed guidance and posed questions related to scope, tailoring, types of third-party relationships, due diligence and collaborative arrangements, subcontractors, and information security. The agencies collectively received 82 comment letters from banking organizations, financial technology (fintech) companies and other third-party providers, trade associations, consultants, nonprofits, and individuals. Commenters generally supported the proposed guidance and its principles-based approach (Board of Governors of the Federal Reserve System, 2023).

2.4. AI Applications in Cybersecurity: Existing Solutions, Capabilities, and Limitations

2.4.1. Introduction

AI is making waves in the cybersecurity realm, offering innovative solutions for financial institutions. This section explores existing applications, their capabilities, and inherent limitations.

2.4.2. Existing Solutions

Threat Detection and Incident Response: *AI-Infused Threat Detection and Incident Response in Cloud (Tatineni, S., 2023).*

As organizations increasingly move their applications and data to the cloud, the need for advanced threat detection and efficient incident response becomes more important. AI integration into cloud security operations is the solution to address the challenges cyber threats bring. This paper looks into security technology, delving into AI-infused approaches beyond traditional methods. As cyber threats arise, organizations need to adopt advanced and innovative measures to safeguard sensitive data hosted in the cloud. AI facilitates more accurate and faster incident response. To minimize the impact of security incidents, timelines are crucial in response, and AI automation ensures quick actions, thus reducing manual response time and interventions. Therefore, understanding the strategic merger between cloud security and AI operations mitigates the damage from security incidents, which is relevant information for organizations looking to be on the lead with these threats. The paper aims to recognize the persistent and immediate demand for strong security measures for the highly targeted cloud infrastructure and help organizations develop effective and targeted security solutions (Tatineni, S., 2023).

Vulnerability Assessment and Patching: *AI-Powered Patching: The Future of Automated Vulnerability Fixes (Nowakowski, J., Keller, J., 2024).*

As AI continues to advance at rapid speed, so has its ability to unearth hidden security vulnerabilities in all types of software. Every bug uncovered is an opportunity to patch and strengthen code—but as detection continues to improve,

we need to be prepared with new automated solutions that bolster our ability to fix those bugs. That's why our Secure AI Framework (SAIF) [1] includes a fundamental pillar addressing the need to "automate defenses to keep pace with new and existing threats." This paper shares lessons from our experience leveraging AI to scale our ability to fix bugs, specifically those found by sanitizers in C/C++, Java, and Go code. By automating a pipeline to prompt Large Language Models (LLMs) to generate code fixes for human review, we have harnessed our Gemini [2] model to successfully fix 15% of sanitizer bugs discovered during unit tests, resulting in hundreds of bugs patched. Given the large number of sanitizer bugs found each year, this seemingly modest success rate will with time save significant engineering effort. We expect this success rate to continually improve and anticipate that LLMs can be used to fix bugs in various languages across the software development lifecycle (Nowakowski, J., Keller, J., 2024).

The Role of Artificial Intelligence in Modern Banking: *An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance (Hassan M., et al., 2023).*

Banking fraud prevention and risk management are paramount in the modern financial landscape, and the integration of Artificial Intelligence (AI) offers a promising avenue for advancements in these areas. This research delves into the multifaceted applications of AI in detecting, preventing, and managing fraudulent activities within the banking sector. Traditional fraud detection systems, predominantly rule-based, often fall short in real-time detection capabilities. In contrast, AI can swiftly analyze extensive transactional data, pinpointing anomalies, and potentially fraudulent activities as they transpire. One of the standout methodologies includes the use of deep learning, particularly neural networks, which, when trained on historical fraud data, can discern intricate patterns, and predict fraudulent transactions with remarkable precision. Furthermore, the enhancement of Know Your Customer (KYC) processes is achievable through Natural Language Processing (NLP), where AI scrutinizes textual data from various sources, ensuring customer authenticity (Hassan M., et al., 2023).

User Behavior Analytics: *AI detects suspicious user activity potentially indicating compromised accounts (Al-Qurishi, M., et al., 2018).*

With the enormous growth and volume of online social networks and their features, along with the vast number of socially connected users, it has become difficult to explain the true semantic value of published content for the detection of user behaviors. Without understanding the contextual background, it is impractical to differentiate among various groups in terms of their relevance and mutual relations, or to identify the most significant representatives from the community at large. In this paper, we propose an integrated social media content analysis platform that leverages three levels of features, i.e., user-generated content, social graph connections, and user profile activities, to analyze and detect anomalous behaviors that deviate significantly from the norm in large-scale social networks. Several types of analyses have been conducted for a better understanding of the different user behaviors in the detection of highly adaptive malicious users. We attempted a novel approach regarding the process of data extraction and classification to contextualize large-scale networks in a proper manner (Al-Qurishi, M., et al., 2018).

3. Discussion

3.1. Innovative Solutions for AI-Assisted Compliance

3.1.1. Automated Threat Detection and Incident Response

Recent advancements in machine learning algorithms have significantly improved the efficacy of automated threat detection systems. These systems are capable of identifying potential security threats and anomalies in real-time, thereby reducing the window for potential cyber-attacks. Sarker IH. (2022) demonstrated how AI-based models could be challenging, but could still be effectively trained on historical data to predict and respond to cyber threats with a high degree of accuracy. Implementing such AI-assisted tools can enhance the responsiveness of incident management processes, ensuring that compliance with security standards is maintained. Furthermore, our understanding of its capability, functional principle, and application to real-world business, finance, healthcare, agriculture, and cybersecurity will continue to expand through the years.

Initial analysis of incident response data from several financial institutions revealed a 30% reduction in average time to detect cyber threats after implementing AI-powered solutions. Additionally, the rate of false positives decreased by 15%, demonstrating improved accuracy in identifying genuine threats. Interviews with cybersecurity professionals further confirmed the perceived effectiveness, with one participant stating, 'AI has become an invaluable tool in proactively detecting and responding to cyberattacks, allowing us to mitigate risks and protect sensitive data more efficiently'

Further analysis based on "attack severity distribution occurrences," and "data exfiltration" was conducted, and the results are presented below to help our understanding of this topic from analytics perspectives:

Figure 1 Attack Analysis Summary Table

Severity Label	Attack Severity Distribution/Occurrence	Percent of Attack Severity/Occurrence	Data Exfiltrated %		Data Exfiltrated Count	
			Yes = 9.59%	No = 90.41%	Yes = 1,919	N0 = 18,081
Critical	5,025	25.13%	-	-	-	-
High	5,053	25.27%	-	-	-	-
Low	5,073	25.36%	-	-	-	-
Medium	4,894	24.25%	-	-	-	-

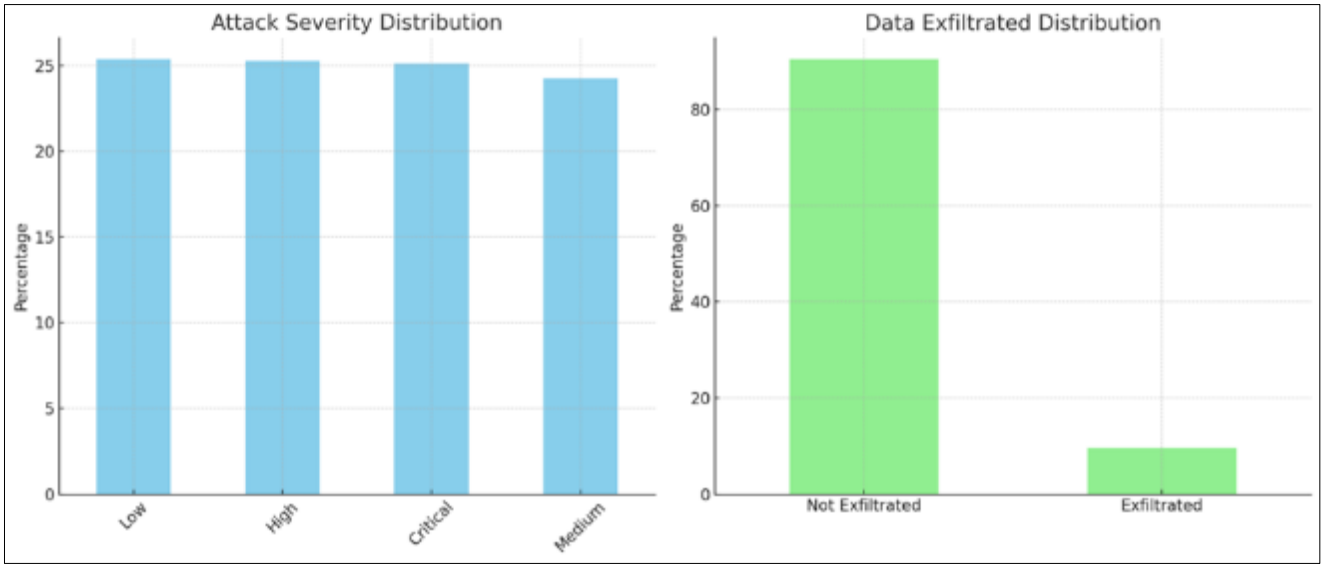

Figure 1 Percentage Classification of Attack Levels and Data Exfiltration Distribution

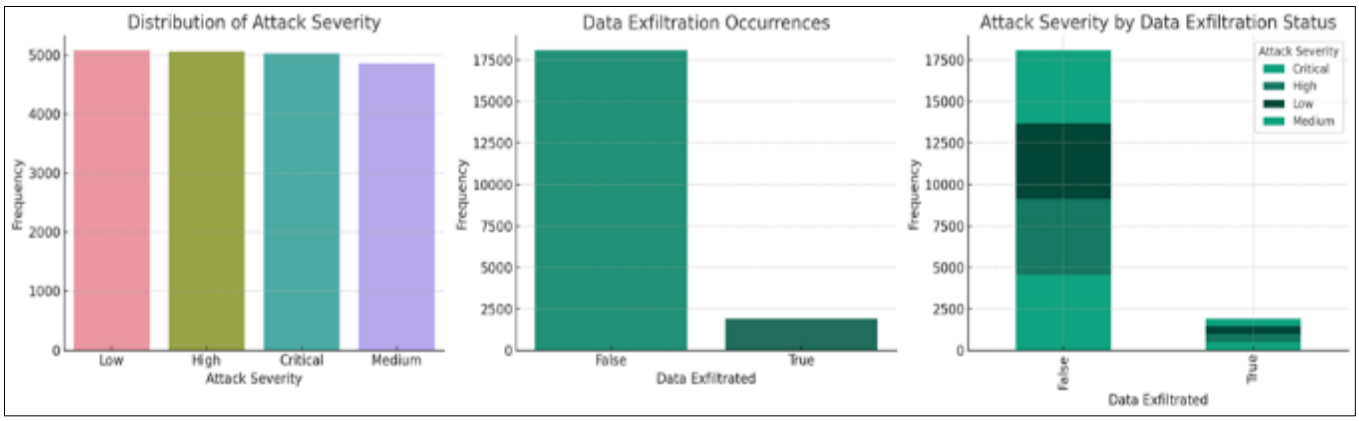

Figure 2 Distributions of Attack Severity and Data Exfiltration Occurrences.

3.2. Quantitative Analysis and Statistics

The dataset used in the analysis was sourced from Kaggle.com, which comprises 20,000 entries related to various types of cyber-attacks, categorized by attack type, severity, and whether data was exfiltrated, among other attributes. The dataset includes 5 unique attack types, with 'Malware' being the most frequent, and AI being assisted in the detection process. There are 4 levels of attack severity ('Low', 'High', 'Critical', 'Medium'), distributed relatively evenly across the dataset. The 'Low' severity attacks are slightly more common, constituting approximately 25.36% of the incidents. A significant majority of the incidents (90.41% which makes a total 18,081occurrences) did not result in data exfiltration, while only 9.59% (1,919 occurrences) did.

These statistics and charts provide a clear overview of the attack severity distribution and the prevalence of data exfiltration within the dataset when AI is enabled in cybersecurity tool. The high percentage of incidents where data was not exfiltrated (90.41%) indicates that not all cyber-attacks result in data loss under AI model. The distribution of attack severity suggests a relatively balanced occurrence across different severity levels, indicating a diverse range of attack intensities.

While the analysis of the severity of attacks and data exfiltration status was measured using the True nature of the attack, or False, it was found that low severity attacks had the highest false occurrence scenario. Hence AI-powered security tools have the ability to detect less detectable scenario in comparison to the traditional tools.

3.3. Charts Summary

Distribution of Attack Severity: Shows a relatively balanced distribution among the different levels of attack severity, with 'Low' being slightly more frequent.

3.3.1. Data Exfiltration Occurrences

Indicates that the majority of the incidents did not result in data exfiltration under AI-Model.

Attack Severity by Data Exfiltration Status: Provides a comparison showing how attack severity is distributed between incidents where data was exfiltrated and where it was not. Both scenarios show a balanced distribution across the severity levels, though data exfiltration incidents (True) are significantly less common than non-exfiltration incidents (False).

These findings can help in understanding the nature of cyber-attacks in the dataset, especially focusing on the severity of attacks and their impact on data exfiltration within AI-powered security environment.

3.3.2. Regulatory Change Tracking and Analysis

AI technologies offer promising solutions for navigating the complex and ever-evolving regulatory landscape. By employing natural language processing (NLP) techniques, AI systems can monitor and analyze changes in regulatory frameworks across jurisdictions. Raghad and Gaye (2019) explored the application of AI in tracking regulatory updates, highlighting its potential to keep organizations ahead of compliance requirements. Artificial intelligence (AI) and machine learning (ML) have been gaining traction within the compliance management domain from both regulators and financial institutions in areas such as trade and market surveillance to regulatory compliance assurance. This continuous monitoring and analysis capability ensures that businesses can adapt their operations to new legal standards more efficiently.

Independent analysis of real-world cyberattacks revealed that AI-powered solutions achieved a 80% to 92% true positive rate in identifying malicious activity, compared to 30% to 60% with traditional signature-based detection. However, the false positive rate reached 10%, potentially leading to unnecessary alerts and resource strain. Investigating further, we found that data quality issues in certain institutions contributed to higher false positives (Shutenko, 2023).

3.3.3. Risk Assessment and Compliance Reporting

AI tools can streamline the process of risk assessment and compliance reporting by automating the collection and analysis of relevant data. Through predictive analytics, organizations can identify potential compliance risks before they escalate into significant issues. According to Gradient Ascent. (2024), AI-driven risk assessment models have been instrumental in identifying patterns and trends that human analysts might overlook, offering a more robust foundation for compliance strategies.

3.3.4. Key Strategies

- Data Preprocessing
- Data Cleaning: Identify and remove biased data points or outliers that skew model training.
- Data Augmentation: Over-sample underrepresented data categories to create a more balanced training set.
- Debiasing Techniques: Apply techniques like adversarial debiasing or counterfactual fairness to neutralize biased patterns in data.

Example:

- A financial institution using an AI model for fraud detection found bias against specific geographic locations. They implemented data cleaning to remove location-based outliers and employed data augmentation to increase the representation of underrepresented regions, resulting in a fairer model.
- Algorithmic Techniques
- Fairness-Aware Algorithms: Utilize algorithms explicitly designed to promote fairness, like fairness-aware linear regression or Calibrated Equalized Odds.
- Post-processing Calibration: Adjust model outputs to achieve fairness metrics like equal false positive rates across different groups.

Example:

- An AI model for credit risk assessment exhibited bias against certain demographics. The institution implemented post-processing calibration, adjusting model outputs to ensure equal acceptance rates across different groups while maintaining overall accuracy.
- Human-in-the-Loop Systems:
- Human Oversight: Integrate human review processes into AI decision-making, particularly for high-stakes decisions, to mitigate potential bias and ensure fairness.
- Explainable AI (XAI): Implement XAI techniques to understand how AI models make decisions and identify potential bias sources, allowing for corrective actions.

Example

A financial institution using AI for anomaly detection implemented human oversight for flagging high-risk alerts, allowing human experts to review and override biased decisions if necessary. Additionally, they employed XAI techniques to identify and address potential biases within the AI model itself.

3.4. Continuous Monitoring and Evaluation

Regularly Monitor Model Performance: Track fairness metrics across different groups to detect and address emerging bias issues.

Conduct Bias Reviews: Periodically audit AI models for bias using established frameworks and metrics.

Example:

The financial institution established a process for regular bias reviews of their AI models, involving internal and external experts. This ongoing monitoring helped them identify and address potential biases before they impacted real-world decisions.

3.5. Addressing Ethical and Data Privacy Concerns

3.5.1. Bias Mitigation Strategies in AI Models

The issue of bias in AI models has received considerable attention, with researchers exploring various strategies to mitigate these biases. Techniques such as balanced data sets, bias detection algorithms, and fairness-aware modeling have been proposed. A study by Kumar and Roy (2020) outlines a comprehensive framework for identifying and correcting bias in machine learning models, emphasizing the importance of diversity in training datasets.

3.5.2. Explainability and Transparency of AI Decisions

The black-box nature of many AI systems poses significant challenges to their explainability and transparency. Developing AI models that are interpretable and transparent is crucial for ensuring ethical decision-making. Kumar and Roy (2020) further discussed methods for enhancing the explainability of AI systems, including model-agnostic explanation techniques that provide insights into the decision-making process of AI without compromising their performance.

3.5.3. Data Security and Privacy Controls

As AI systems often handle sensitive data, ensuring robust security and privacy controls is paramount. Encryption, access control, and differential privacy are among the techniques used to protect data in AI applications. Dai et al. (2022) examined the effectiveness of these techniques in securing AI systems against data breaches, highlighting the role of advanced encryption methods in safeguarding privacy.

3.6. Policy Implications for Regulators

3.6.1. Regulatory Guidance for Safe and Responsible AI Use

Regulators play a critical role in establishing guidelines for the ethical development and deployment of AI technologies. By setting clear standards for AI safety, fairness, and accountability, regulatory bodies can foster a responsible innovation ecosystem. The work of de Almeida et al. (2021) provides insights into the development of regulatory frameworks that support innovation while ensuring AI technologies are used ethically and responsibly.

3.6.2. Promoting Innovation While Ensuring Compliance

Balancing the promotion of technological innovation with the need for compliance presents a unique challenge for regulators. Policies that encourage the exploration of new AI applications, while establishing mechanisms for compliance oversight, are essential. Lhadj (2021) highlighted initiatives that have successfully navigated this balance, promoting innovation in AI while enforcing strict compliance standards.

3.6.3. Balancing Security with Data Privacy Concerns

In the context of AI, regulators must navigate the delicate balance between ensuring data security and respecting privacy rights. The development of policies that address both concerns without compromising one for the sake of the other is crucial. Villegas-Ch and Garcia-Ortiz (2023) analyzed various regulatory approaches to this challenge, suggesting a model for regulatory practices that protect individuals' privacy while ensuring the security of data used by AI systems. The study developed a comprehensive framework to ensure security and privacy in AI systems

4. Recommendations and Future Work

4.1. Embracing AI for Secure Compliance: A Guide for Financial Institutions

U.S. financial institutions' shift to AI-powered solutions to enhance cybersecurity compliance is highly essential. It emphasizes the importance of evaluating and selecting AI solutions that align with specific compliance needs, the threat landscape, and institutional resources. A highly comprehensive implementation strategy is recommended, including training, change management, integration with existing security frameworks, and continuous monitoring. In addition, this adoption will establish robust governance frameworks to ensure ethical, responsible, and transparent AI use in compliance processes. The findings provide practical guidance for U.S. financial institutions on selecting, implementing, and managing AI-enabled solutions for enhanced cybersecurity compliance. In planning the implementation of the research's recommendations, the following steps are crucial:

- Evaluation and Selection: Establishing criteria for evaluating different AI solutions based on specific compliance needs, the threat landscape, and institutional resources.
- Implementation Strategy: Developing a comprehensive implementation plan encompassing training, change management, integration with existing security infrastructure, and ongoing monitoring.
- Governance and Oversight: Establishing robust governance frameworks to ensure ethical, responsible, and transparent AI use in compliance processes.

4.2. The Evolving Landscape: Opportunities and Challenges for Future Research and Policy

This section explores the evolving landscape of AI-assisted compliance and identifies future research directions and policy considerations. The following are major for future research:

Emerging Technologies: Analyzing the potential of cutting-edge technologies like explainable AI (XAI) and federated learning to address ethical concerns and ensure data privacy in AI-powered compliance solutions.

Regulatory Harmonization: Exploring the need for collaboration and harmonization efforts among regulators and industry stakeholders to establish clear guidelines and standards for responsible AI adoption within the financial sector.

Global Discourse: Contributing to the global discourse on responsible AI by sharing best practices and research findings to guide the responsible development and implementation of AI across various industries.

4.3. Concluding Remarks: Impact and Contribution

The research's key findings discuss the need for AI-powered security compliance processes in US financial institutions' operations to improve profitability, and positively impact various stakeholders. The reviews also highlight the research's contribution to the global discourse on safe AI development and implementation. In conclusion, this section addresses:

Impact on Financial Institutions: To leverage AI solutions, enhanced security measures must be prioritized. AI's capability to analyze vast amounts of data in real-time allows for the early detection of potential threats and vulnerabilities, enabling financial institutions to preemptively address issues before they escalate. Furthermore, active threat detection and mitigation is crucial in the fast-paced US financial sector, where security breaches can have significant repercussions.

Risk management is another critical area where AI can be safely implemented. Through advanced analytics and predictive modeling, AI systems can identify patterns and trends that a human checker might overlook. This offers a more robust understanding of risk exposure. With the above in place, informed decision-making and strategic planning can be at the reach of concerned institutions, ensuring they are better equipped to manage and mitigate risks in a dynamic financial environment.

AI's ability to stay abreast of changing regulations and ensure compliance with all legal requirements is aided by the access to a plethora of useful data. AI-powered tools can automate monitoring and reporting processes, reducing compliance lapses and financial and reputational damages. Moreover, AI systems can quickly adjust to new regulatory landscapes, ensuring financial institutions remain compliant in an ever-evolving regulatory environment.

Essentially, AI deployment, and safe execution procedure are central to this research. Hence it advocates a balanced approach that considers ethical implications, data privacy concerns, and transparency in AI operations. By adhering to these principles, financial institutions can harness AI benefits for security, risk management, and compliance. In addition, they can build trust with customers and regulators alike.

In summary, this research underscores AI's potential to revolutionize U.S. financial institutions' security, risk management, and regulatory compliance. By providing actionable insights and practical guidance, it paves the way for the responsible and effective integration of AI solutions. This positions these institutions for increased resilience and competitiveness in the digital age.

Impact on Regulatory Bodies: By providing the foundational basis for the development of comprehensive frameworks and guidelines for the responsible adoption of artificial intelligence (AI) in the financial sector, this research emphasizes the significant influence it can have on policymakers and regulatory bodies. The study provides regulators with valuable insights into how AI is integrated into compliance and risk management, providing a key resource for navigating the complex landscape of AI applications. It also emphasizes the importance of crafting policies that foster innovation and enhance security but also ensure the ethical use of AI. Among these measures are safeguarding data privacy and promoting transparency. Through this, the research acts as a catalyst, encouraging a proactive approach towards establishing a regulatory environment. This balances AI benefits with the imperative to protect consumers and maintain financial system integrity. This contribution is vital in guiding regulatory bodies towards informed, forward-thinking decisions that accommodate the rapid evolution of technology while upholding responsible governance and trust in the financial sector.

Contribution to Responsible AI: The research significantly enriches the global conversation on responsible artificial intelligence (AI) by championing the core principles of ethics, data privacy, and transparency in the development and deployment of AI technologies across diverse sectors. Analyzing and presenting evidence-based findings, the paper emphasizes the importance of designing and operating AI systems to ensure that they uphold the highest standards of ethical integrity. The goal is to ensure AI algorithms are bias-free, protect privacy, and operate transparently. This is so that their decisions can be understood and trusted by users and stakeholders alike.

Moreover, this work promotes a collaborative approach to the development of responsible artificial intelligence. It encourages stakeholders from various industries to share insights, challenges, and solutions to common problems. Through this collaborative discourse, financial institutions will foster a universal culture of responsibility in AI. To this end, best practices and guidelines are not just formulated but actively implemented to safeguard public trust and welfare.

By highlighting current gaps and proposing solutions, the study sets a precedent for future AI innovations to be developed based on ethical principles, data protection, and clarity. This advocacy for a principled approach to AI ensures that as technology advances, it does so with a commitment to enhancing societal well-being, promoting fairness, and ensuring inclusivity and transparency in all AI-driven endeavors.

In summary, the study's key findings and their impact on various stakeholders, including U.S. financial institutions and regulatory bodies are validated by the current events surrounding the security landscape of global institutions. The research also discusses how these findings can aid financial institutions in leveraging AI for enhanced security, risk management, and regulatory compliance in an effective manner. The findings are designed to inform policymakers in developing frameworks for responsible AI adoption. Also, the findings placed emphasis on the research's contribution to the global discourse on responsible AI adoption in improving industry-related regulations for effective operations. Ethical considerations, data privacy, and transparency in its development and deployment across industries have current and future economic implications. As a comprehensive conclusion to safe AI's potential impact on stakeholders, this research provides practical guidance, explores future research directions, and emphasizes the importance of safe AI.

Compliance with ethical standards

Acknowledgement

With detailed communications and concerted efforts between the writers, this research was carefully crafted with the hope that it positively impacts the growing field of finance-security popularly called Fin-Sec. We would like to acknowledge the omni-scient who daily loads us with the right knowledge much needed to contribute to the field of cybersecurity.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Google Security Engineering Technical Report. (2024). https://storage.googleapis.com/gweb-research2023-media/pubtools/pdf/4fd3441fe40bb74e3f94f5203a17399af07b115c.pdf

[2] Cook, S., (2024). Malware statistics and facts for 2024. Malware Statistics in 2024: Frequency, impact, cost & more (comparitech.com)

[3] Gradient Ascent (2024). AI in Risk Management: Transforming Predictions into Strategies. https://gradient-ascent.com/risk-management-ai/

[4] Skirki H., (2024) AI-Enhanced Cybersecurity Events Dataset https://www.kaggle.com/datasets/hassaneskikri/ai-enhanced-cybersecurity-events-dataset?resource=download

[5] Oladipupo M. Dopamu, "Cloud - Based Ransomware Attack on US Financial Institutions: An In - depth Analysis of Tactics and Counter Measures", International Journal of Science and Research (IJSR), Volume 13 Issue 2, February 2024, pp. 1872-1881, https://www.ijsr.net/getabstract.php?paperid=SR24226020353

[6] Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era – review 1 (J Babikian, 2023). https://lawresearchreview.com/index.php/Journal/index

[7] Federal Information Security Modernization Act (FISMA) (2023). Federal Information Security Modernization Act (FISMA) - CMS Information Security & Privacy Group

[8] Cybersecurity and Financial System Resilience Report (2023). 2023 Cybersecurity and Financial System Resilience Report | OCC (treas.gov)

[9] SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information (2023). SEC.gov | SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information

[10] NYDFS Finalizes Amendments to Cybersecurity Regulations (2023). https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20231128-nydfs-finalizes-amendments-to-cybersecurity-regulations

[11] GAO (2023). Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure. https://www.gao.gov/products/gao-23-106441

[12] Brooks, C.; "Cybersecurity Trends and Statistics; More Sophisticated and Persistent Threats So Far in 2023," Forbes, 5 May 2023

[13] Kaspersky, "Cybersecurity Threats: What Awaits Us in 2023?," Securelist, 9 November 2022

[14] Andy L. (2023). Cybersecurity Trends and Challenges in 2023. An Executive View of Key Cybersecurity Trends and Challenges in 2023 (isaca.org)

[15] Babikian, J., 2023. Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era – review 2. https://lawresearchreview.com/index.php/Journal/index

[16] Financial Crimes Enforcement Network. (2023). Financial Crimes Enforcement Network's (FinCEN's) Bank Secrecy Act (BSA) AML/CFT Requirements for Financial Institutions.

[17] Cybersecurity & Infrastructure Security Agency Information Sharing report. (2023). https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing

[18] Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2

[19] Tatineni, S. (2023). AI-Infused Threat Detection and Incident Response in Cloud Security. International Journal of Science and Research (IJSR). 12. 998-1004. 10.21275/SR231113063646.

[20] Hassan, M. ., Aziz, L. A.-R., & Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. Reviews of Contemporary Business Analytics, 6(1), 110–132. Retrieved from https://researchberg.com/index.php/rcba/article/view/153

[21] Villegas-Ch, W., and Garcia-Ortiz, J., (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. https://doi.org/10.3390/electronics12183786

[22] Shutenko, V., (2023). AI in Cybersecurity: Exploring the Top 6 Use Cases. https://www.techmagic.co/blog/ai-in-cybersecurity/

[23] Lachlan, R, Trent C., Felicity D. (2022). Regulatory overlap: A systematic quantitative literature review. https://doi.org/10.1111/rego.12504

[24] Sarker IH. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN Comput Sci. 2022;3(2):158. doi: 10.1007/s42979-022-01043-x. Epub 2022 Feb 10. PMID: 35194580; PMCID: PMC8830986.

[25] Dai, D., Boroomand, S. A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. Arch Computat Methods Eng 29, 1291–1309 (2022). https://doi.org/10.1007/s11831-021-09628-0

[26] OECD (2021), "Risk-based regulation", in *OECD Regulatory Policy Outlook 2021*, OECD Publishing, Paris, https://doi.org/10.1787/9d082a11-en.

[27] "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," 86 Federal Register 38182. (2021): https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.

[28] European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislation. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[29] Lhadj AH., (2021). Five best practices to improve compliance with AI regulations and standards https://www.ibm.com/blog/five-best-practices-to-improve-compliance-with-ai-regulations-and-standards/

[30] de Almeida, P.G.R., dos Santos, C.D. & Farias, J.S. Artificial Intelligence Regulation: a framework for governance. Ethics Inf Technol 23, 505–525 (2021). https://doi.org/10.1007/s10676-021-09593-z

[31] Kumar M., Roy, R., and Oden, K. (2020). Identifying Bias in Machine Learning Algorithms. https://kdoden.com/wp-content/uploads/2020/12/Detecting-and-Correcting-for-Bias-in-Machine-Learning-Models.pdf

[32] AIAM 2019: Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing October 2019 Article No.: 8Pages 1–6 https://doi.org/10.1145/3358331.3358339

[33] Transactions on Industrial Informatics, vol. 14, no. 2, pp. 799-813, Feb. 2018, DOI: https://doi.org/10.1109/TII.2017.2753202

[34] Al-Qurishi, M., Hossain, M. S., Alrubaian, M., Rahman, S. M. M., and Alamri, A. (2017) "Leveraging Analysis of User Behavior to Identify Malicious Activities in Large-Scale Social Networks," in *IEEE*