Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7, 2222-2245
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i7.9142

Enhancing financial information security through advanced predictive analytics: A PRISMA based systematic review

Md Nazmul Hasan[1], Md Saidul Islam Papel[2], Imran Hossain Rasel[3], Sadia Akter[4], Mst Khadiza Aktar[5], Md Zainal Abedin[6], Lisa Mani[7*]

[1]MS in Business Analytics, University of New Haven, West Haven, Connecticut, United States; mhasa9@unh.newhaven.edu (M.N.H.)
[2]MBA-MIS, International American University (IAU), 3440 Wilshire Blvd STE 1000, Los Angeles, CA 90010, United States; mdpapeldu@gmail.com (M.S.I.P.)
[3]MS in Business Analytics, University of New Haven, Connecticut, United States; irase1@unh.newhaven.edu (I.H.R.)
[4]Masters of Business Administration in Management Information Systems, International American University, Los Angeles, California United States; sadia03.akter@gmail.com (S.A.)
[5]Department of Business Administration (Major in Accounting and Information Systems), Shahjalal University of Science & Technology, Sylhet-3114, Sylhet, Bangladesh; khadiza.lucky.bus@gmail.com (M.K.A.).
[6]Department of Business Administration, Z.H Sikder University of Science and Technology, Shariatpur, Bangladesh; mabed099@uottawa.ca (M.Z.A.).
[7]Department of Business Administration, Finance and Banking, Shahjalal University of Science and Technology, Sylhet 3114, Sylhet, Bangladesh; lisamoni00@gmail.com (L.M.).

Abstract: The rapid digital transformation of the financial sector has escalated cybersecurity challenges, necessitating advanced solutions to protect sensitive data and mitigate cyber threats. This study systematically reviews the application of advanced predictive analytics, powered by artificial intelligence (AI) and machine learning (ML), in enhancing financial information security. Predictive analytics enables financial institutions to proactively detect fraud, assess risks, monitor behavioral anomalies, and anticipate emerging cyber threats by analyzing vast historical and real-time data through a PRISMA-based systematic review. Key applications include real-time fraud detection, dynamic risk management, cyber threat intelligence, and ensuring data integrity from 555 previous studies across various databases such as Scopus, Web of Science, DOAJ, Google Scholar, ResearchGate, and PubMed. Additionally, 63 studies and 12 reports were finalized to address research gaps. Despite significant advancements, challenges remain regarding integration with legacy systems, data privacy compliance under regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), model robustness against adversarial attacks, and workforce skill shortages. Emerging trends such as blockchain integration, quantum-safe cryptography, privacy-preserving techniques like federated learning, and AI-driven security automation show promise for future developments. The study emphasizes the critical need for transparent, explainable predictive models and interdisciplinary collaboration to bridge existing gaps. Ultimately, leveraging advanced predictive analytics is vital for strengthening financial cybersecurity frameworks, ensuring regulatory compliance, and maintaining market stability in an increasingly complex and data-driven financial ecosystem. Continued innovation and research are essential to fully realize these benefits and address evolving threats.

Keywords: *Artificial intelligence (AI), Data privacy, Financial information security, Fraud detection, Machine learning (ML), Predictive analytics, PRISMA, Systematic review.*

1. Introduction

In the current landscape characterized by data, sophisticated predictive analytics has emerged as a crucial instrument utilized across various sectors, such as finance, healthcare, marketing, and cybersecurity [1]. Utilizing historical data, statistical algorithms, and machine learning techniques,

History: Received: 13 May 2025; Revised: 18 June 2025; Accepted: 23 June 2025; Published: 28 July 2025
* Correspondence: lisamoni00@gmail.com

predictive analytics empowers organizations to anticipate future outcomes and make well-informed decisions. This approach allows businesses to take proactive measures, identifying potential risks and opportunities before they arise, rather than relying solely on reactive strategies. In the financial sector, predictive analytics is reshaping how institutions assess risk, detect fraud, and manage investments [2]. By analyzing vast amounts of transactional data, market trends, and consumer behavior, financial institutions can uncover hidden patterns that traditional analysis might miss, providing valuable insights for timely decision-making [3].

Financial information security refers to the practices, policies, and technologies employed by financial institutions to protect sensitive data from unauthorized access, cyberattacks, and other malicious activities [4]. As financial transactions and sensitive information increasingly move into digital spaces, ensuring the confidentiality, integrity, and availability of financial data becomes a growing challenge. Financial institutions are prime targets for cybercriminals because of the large volume of valuable information they store, ranging from personal customer details to financial assets [5].

We live in a time dominated by digital technology, which, like any other innovation, offers both advantages and challenges [6]. A significant issue is the security risk involved. As more sensitive data moves online, the number and severity of security breaches continue to rise. Cybercriminals are becoming more adept at avoiding detection, with newer malware programs already using tactics to bypass antivirus systems and other security measures [7]. Cybersecurity, however, is at a critical juncture, and future research should prioritize developing predictive systems for cyber-attacks, capable of forecasting key events and consequences, instead of relying solely on reactive defense strategies focused on damage control [8]. There is a global need for systems that can deliver an all-encompassing, predictive analysis of cyber risks. Essential cybersecurity functions, such as prediction, prevention, detection, and incident response, should be automated and carried out with intelligence. Artificial Intelligence (AI), especially through Machine Learning (ML), has the capability to identify patterns and forecast future behaviors based on historical data, thus aiding in the prevention or identification of potentially malicious actions, which is the central theme of this study [9].

Within the financial services sector, the application of machine learning is crucial for enhancing predictive analytics [10]. Machine learning algorithms, including decision trees, neural networks, and regression analysis, analyze complex data and uncover trends, which are subsequently utilized to forecast future occurrences, such as fraudulent activities or market changes. These predictive models help in real-time fraud detection, credit scoring, and portfolio management, improving financial security [11]. However, implementing predictive analytics comes with challenges, including balancing predictive accuracy with compliance to privacy regulations like GDPR and CCPA [12]. It is essential for financial institutions to maintain the quality and integrity of their data, as any inaccuracies can significantly compromise the reliability of predictions [13]. With the ongoing evolution of AI, its influence in predictive analytics is set to grow, allowing financial institutions to enhance the accuracy of their predictions. However, the incorporation of AI and ML into current systems presents difficulties, including issues related to model explainability and safeguarding against adversarial attacks [14]. Despite these challenges, predictive analytics is crucial in modern financial services, and its continued development promises to enhance decision-making, risk management, and security.

The rapid digital transformation of financial services has introduced both opportunities and risks. While innovations such as online banking, mobile payments, and digital wallets have enhanced convenience and accessibility, they have also broadened potential vulnerabilities for breaches. Cybercriminals are employing more advanced techniques, including phishing, malware, and ransomware attacks, to exploit vulnerabilities in financial systems. Furthermore, the rise of insider threats and data breaches has amplified the urgency for robust security measures [15]. In response to these challenges, financial institutions are increasingly integrating predictive analytics into their security systems [16]. These tools enable organizations to detect unusual patterns, predict potential fraud, and respond quickly to emerging threats. Machine learning models, for example, can continuously learn from historical data to identify and predict risks with high accuracy [17].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Despite the increasing adoption of predictive analytics in the financial sector, several research gaps still remain, particularly in examining the changing landscape of cybersecurity threats. One major gap is the challenge of integrating predictive analytics with existing legacy systems in financial institutions [18]. Machine learning and AI algorithms play a vital role in identifying fraud and overseeing risks, they must be seamlessly integrated with traditional systems that are often outdated and lack the necessary infrastructure to support advanced analytics [19]. This integration is complex and requires significant investment in both time and resources, making it a critical area for research. Additionally, while predictive analytics is designed to anticipate risks, the ability to predict novel or sophisticated cyber-attacks, especially those driven by adversarial machine learning, remains an open challenge. Further investigation is essential to create resilient models capable of adjusting to new, previously unseen threats without relying on historical patterns [20].

Furthermore, the importance of data privacy and regulatory compliance are significant concerns when implementing predictive analytics in financial information security. The growing use of personal data in machine learning models raises inquiries regarding the ethical ramifications and privacy issues, especially in jurisdictions with stringent Legislation regarding data protection, including the GDPR as well as the CCPA [21]. There exists a necessity for research on how to assure compliance with these regulations while still maintaining the effectiveness of predictive models [22]. Additionally, it is essential to improve the transparency and clarity of AI models because financial institutions need to trust the predictions made by these systems and understand the reasoning behind them [23]. This gap in explain ability also elicits apprehensions regarding the interpretability of the models in cases of audits or investigations. Research into improving the interpretability of AI models while maintaining their accuracy is necessary to ensure their broader acceptance and deployment in the financial sector. The following research objectives were conducted on previous studies.

RO1: Develop effective models that integrate predictive analytics with legacy financial systems.

RO2: To improve the Robustness of Predictive Models Against Emerging and Adversarial Cyber Threats

RO3: This research aims to explore methods for ensuring data privacy and regulatory compliance in financial predictive models.

2. Literature Review

In recent years, the integration of advanced predictive analytics in financial information security has become a crucial area of research, as the financial sector faces increasing threats from cybercrime, fraud, and data breaches. Predictive analytics, utilizing machine learning (ML) and artificial intelligence (AI), has the potential to significantly enhance the way financial institutions identify risks, manage security breaches, and assess vulnerabilities in their systems. The emergence of these technologies has transformed how financial organizations can proactively address cybersecurity challenges, making predictive tools a key part of their security infrastructures [9]. A major benefit of predictive analytics in financial security is its capability to detect anomalous behavior in real-time, which is crucial in preventing cyberattacks before they escalate [7]. By applying ML algorithms to large volumes of data, financial institutions can analyze transaction patterns, identify potential fraud, and predict cyber threats, enabling them to mitigate risks effectively and swiftly [21].

The conduct of predictive analytics in detecting fraud is particularly important in the digital finance ecosystem. As financial institutions increasingly rely on digital transactions, the need for robust fraud detection systems has grown [11]. Advanced machine learning algorithms evaluate patterns in client behavior and transaction data, facilitating the identification of fraudulent actions that may not be evident through conventional security measures. Predictive models can identify questionable transactions in real time, enabling financial institutions to intervene before fraud inflicts substantial harm [1]. Similarly, in risk management, AI-driven models help predict probable market changes and identify high-risk investments, providing decision-makers with the necessary tools to make better-informed and secure financial decisions [2]. Furthermore, by utilizing big data analytics, predictive models can also enhance

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

decision-making in credit scoring, loan approvals, and market forecasting, which are essential to financial services [10].

Table 1.
Summary of previous Studies on Advanced Predictive Analytics for Financial Information Security.

Study	Focus Area	Key Findings
Braun, et al. [6]	Challenges of security and privacy in smart cities	The article highlighted predictive models as vital for cybersecurity risk mitigation, stressing the need for proactive systems.
Aslan, et al. [7]	Cybersecurity vulnerabilities and solutions	The article highlighted the application of predictive analytics to identify and alleviate cyber dangers within financial institutions.
Sarker [9]	Machine learning in cybersecurity	The presentation demonstrated the role of machine learning in real-time threat identification and fraud mitigation within the financial services industry.
Javaid [2]	AI-driven predictive analytics in finance	The study demonstrated how AI improves risk assessment and decision-making, emphasizing the challenges of predictive model integration.
Williams, et al. [11]	ML for fraud detection in digital finance ecosystems	ML models can proactively identify fraudulent patterns and reduce financial losses.
Munir, et al. [12]	Data privacy and compliance in AI systems	Highlighted challenges of GDPR and CCPA compliance in AI-based predictive analytics for financial security.
Baniecki and Biecek [14]	Adversarial attacks in AI models	Discussed vulnerabilities in AI models and need for robustness against adversarial threats in financial systems.
Al Mahmud, et al. [4]	Financial information security threat evaluation	Reviewed cybersecurity risks and evaluated predictive analytics as a tool for banking system protection.

While predictive analytics offers considerable advantages, challenges remain, especially regarding data privacy and regulatory compliance. Financial institutions must balance the effectiveness of predictive models with the need to adhere to rigorous standards, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [12]. The regulations establish rigorous standards for the collection, processing, and storage of customer data, making it imperative for predictive models to operate within these boundaries without compromising on performance. Research by Baniecki and Biecek [14] highlights the growing concern regarding the implications of data privacy within artificial intelligence and machine learning, where the transparency of decision-making processes remains a key challenge. Financial organizations need to ensure that their predictive models are explainable and comply with privacy regulations, all while maintaining their predictive capabilities. Consequently, there is an increasing demand for research on privacy-preserving techniques in machine learning, including federated learning and differential privacy, which can assist financial institutions in developing secure and compliant predictive models [12].

Moreover, the dynamic landscape of cyber-attacks presents an additional challenge for predictive analytics in financial information security. Conventional machine learning models depend significantly on past data for predictions; however, this method tends to falter when confronted with novel or complex threats [6]. Adversarial attacks, in which malicious entities alter input data to mislead predictive models, are increasingly becoming a significant issue in the realm of AI-driven cybersecurity. According to the findings of Baniecki and Biecek [14] adversarial attacks significantly compromise the reliability of AI systems, thereby challenging the trustworthiness of predictions in critical financial contexts. Therefore, research into developing more robust and resilient predictive models is necessary to enhance the identification and mitigation of emerging cyber threats. With the ongoing advancements in AI and machine learning technologies, financial institutions must adopt more sophisticated and adaptive models that can handle these evolving challenges and remain effective in an ever-changing cybersecurity landscape [8].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Table 2.
Types, Applications, and Preventive Actions of Financial Information Security.

Types of Financial Information Security	Prospective Applications	Preventive Actions	Source
Fraud Detection	Machine learning models identify atypical patterns in financial transactions to mitigate fraudulent activities as they occur. These models can continuously improve by learning from historical data, helping institutions predict future fraudulent behaviors.	Implement machine learning-based fraud detection systems to flag suspicious transactions and reduce the potential for deceptive practices.	Ashfaq, et al. [24]
Risk Management	Models utilizing artificial intelligence evaluate the potential risks associated with transactions, investments, or customers by analyzing past behavior and market trends, assisting financial institutions in making informed decisions and preventing high-risk activities.	Establish AI-driven risk assessment models to continuously monitor transaction patterns and provide alerts for potential high-risk activities.	Williams, et al. [11]
Behavioral Analytics	Predictive analytics models monitor user behavior and detect abnormal activities such as unusual logins, transactions, or access patterns to prevent identity theft or account takeovers.	Deploy behavioral analytics solutions to detect deviations from regular user behavior and prevent unauthorized access or identity theft.	Shah, et al. [25]
Cyber Threat Intelligence	Artificial intelligence systems forecast possible cyber-attacks through the examination of network traffic patterns, historical attack information, and external threat intelligence, enabling financial institutions to adopt proactive measures and reduce cyber risks.	Employ predictive models for cyber threat intelligence to pinpoint vulnerabilities and proactively address potential cyber-attacks before they manifest.	Yeboah-Ofori, et al. [26]
Encryption	Encryption methods safeguard sensitive financial information by transforming it into an unreadable format, thereby ensuring data privacy and confidentiality throughout transmission or storage.	Implement end-to-end encryption protocols to secure data during transmission and protect customer information from interception.	Karbasi and Shahpasand [27]
Access Control	Access control mechanisms ensure that only authorized personnel can access specific financial information, preventing unauthorized access and reducing the risk of data breaches.	Enforce strict access control policies, ensuring that only authorized personnel can access critical financial systems and data.	Ward and Smith [28]
Network Security	Network security measures, including firewalls, intrusion detection systems, and secure communication protocols, help prevent unauthorized access and cyber-attacks on financial institutions' networks.	Use firewalls, intrusion detection systems, and secure communication protocols to safeguard financial institutions' networks from cyber threats.	Qasaimeh, et al. [29]
Data Integrity	Data integrity solutions ensure that financial data is accurate, consistent, and reliable by detecting and preventing unauthorized alterations or corruptions.	Establish protocols for data integrity and conduct regular audits to maintain the accuracy of financial data and protect it from unauthorized alterations.	Sabale, et al. [30]

3. Research Methodology

The PRISMA 2020 methodology is widely acknowledged as the benchmark framework for the execution and documentation of systematic reviews and meta-analyses. For this research on "Advanced Predictive Analytics in Financial Information Security," A comprehensive analysis will be undertaken following the PRISMA 2020 guidelines to assess the various predictive analytics techniques used in financial security, including machine learning, AI, and big data analytics [21]. The systematic review will help synthesise existing studies on how predictive models are applied in fraud detection, risk management,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

and cybersecurity and the challenges related to their implementation. The following steps, based on PRISMA 2020 guidelines, was followed for the methodology:

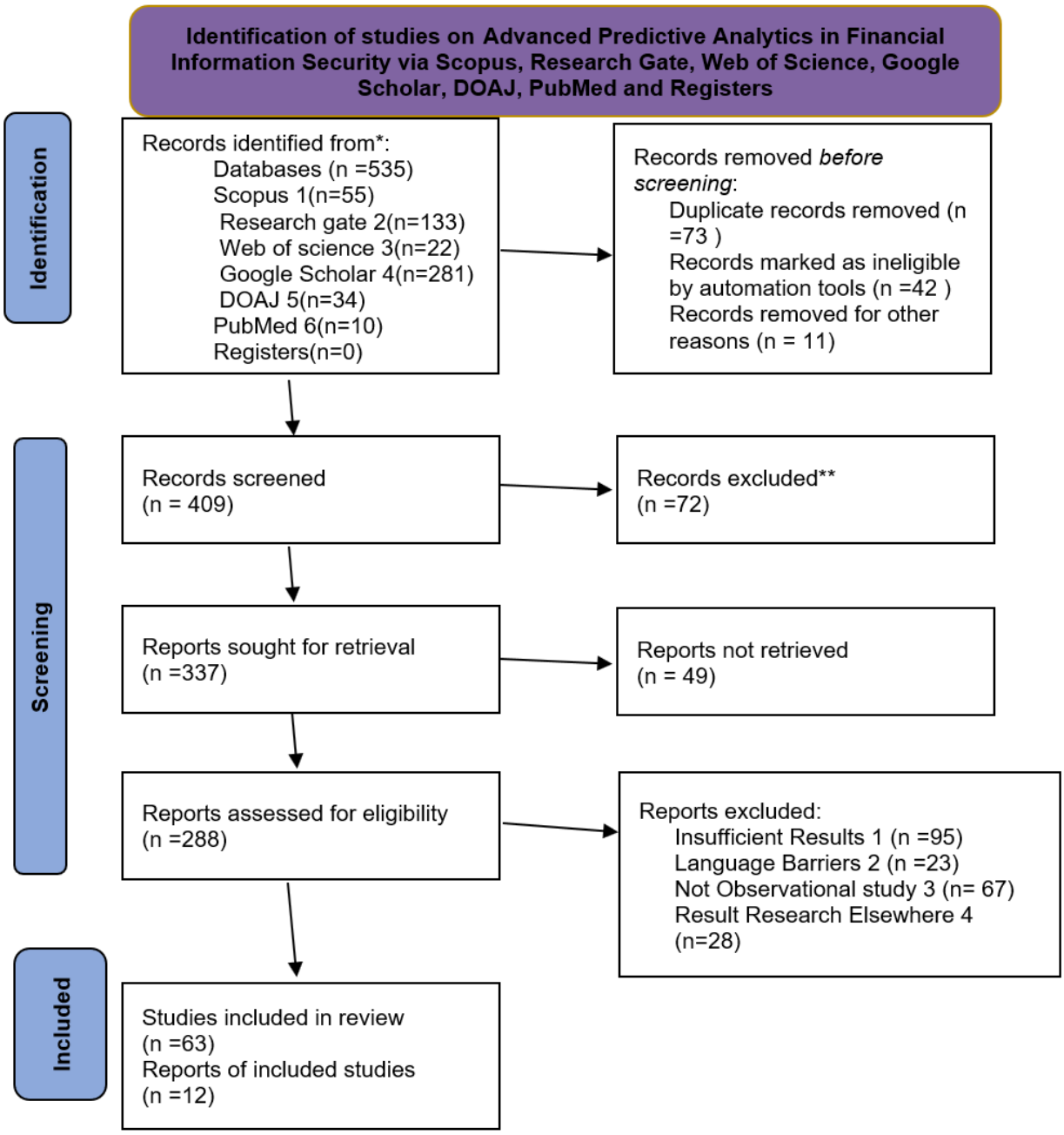

Figure 1.
PRISMA based systematic review.

3.1. Identification of Studies

The identification phase of this systematic review involved conducting a comprehensive search across multiple academic databases to gather relevant studies on advanced predictive analytics in financial information security. The databases used for the search were Scopus, ResearchGate, Web of Science,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Google Scholar, DOAJ, and PubMed. The search yielded a total of 535 records, with contributions from various sources: Scopus (n = 55), ResearchGate (n = 133), Web of Science (n = 22), Google Scholar (n = 281), DOAJ (n = 34), and PubMed (n = 10). No records were identified through registers, indicating that most relevant articles came from these established academic sources.

3.2. Screening

After the removal of duplicate and ineligible 409 records were screened for this research topic. Reports excluded were those with insufficient results (95 records), language barriers (23 records), Not Observational study (67 records), and Result Research Elsewhere (28 records). As a result of this process, 288 reports were evaluated for their eligibility

3.3. Eligibility Assessment

The 288 reports were assessed for eligibility, and after evaluation, the final selection was narrowed down to 63 eligible studies.

3.4. Inclusion

Out of the 63 studies evaluated, 12 were chosen for the final evaluation based on their significance and methodological rigor.

3.5. Previous Studies Supporting Methodology

Previous studies have employed similar methodologies in their systematic review of the application of predictive analytics in financial information security, which validates the effectiveness of the PRISMA framework for data synthesis and analysis [21]. These studies underscore the growing favor of predictive models as well as machine learning (ML) techniques to detect financial fraud, assess cybersecurity risks, and enhance decision-making within financial institutions. Braun, et al. [6] used a systematic review approach to investigate cybersecurity threats in smart cities, emphasizing the role of predictive models in mitigating risks, similar to how predictive analytics in financial security aims to improve fraud detection and risk management Mimi and Mani [31]. Aslan, et al. [7] applied PRISMA in their review of cybersecurity vulnerabilities, showing the framework's utility in assessing predictive analytics methodologies used in financial security. Sarker [9] also followed the PRISMA approach in his review of applications of machine learning in cybersecurity, stressing the importance of predictive analytics for detecting fraud and securing financial systems. Similarly, Javaid [2] demonstrated how a PRISMA-based systematic review could evaluate the influence of AI-driven predictive models on the evolution of financial risk assessment, confirming the relevance and effectiveness of this methodology for synthesizing studies on financial information security.

3.6. Justification for Using the PRISMA Methodology

The PRISMA framework is highly suited for this study due to its distinct advantages:

1. Comprehensive Literature Integration: It allows for the inclusion of all relevant studies, providing a thorough understanding of AI's impact on marketing automation [9].
2. Increased Transparency and Replicability: The structured nature of the PRISMA approach ensures clarity, facilitating replication and verification of results by other researchers [32].
3. Rigorous Quality Assurance: PRISMA emphasises the inclusion of only high-quality and pertinent research, minimising the potential for biases and improving the reliability of the findings [33].

4. Discussion

The discussion section of this study encompasses a comprehensive examination of multiple critical components of financial information security through the lens of predictive analytics [34]. It includes detailed analyses of fraud detection mechanisms, risk management strategies, and behavioral analytics

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

tools, all powered by AI and machine learning [35]. Additionally, the role of cyber threat intelligence in proactively identifying emerging threats is explored, alongside the importance of network security protocols and data integrity frameworks. Each topic is evaluated in terms of its practical application, technological challenges, regulatory considerations, and future implications. This multifaceted discussion provides a holistic understanding of how advanced predictive analytics can enhance security, compliance, and resilience in the digital financial ecosystem.

4.1. Fraud Detection in Financial Information Security

Fraud detection is a crucial aspect of financial information security, particularly in the current digital and data-driven financial ecosystem [36]. With the rise of online banking, mobile payments, and digital financial services, the volume and complexity of transactions have soared, providing fertile ground for fraudulent activities. The incorporation of sophisticated predictive analytics, driven by machine learning (ML) and artificial intelligence (AI), has transformed fraud detection in financial systems [37]. Predictive algorithms can evaluate extensive transactional data in real-time, detecting anomalous or suspicious trends that may signify fraudulent activity [38]. Machine learning algorithms, including decision trees, neural networks, and anomaly detection models, are engineered to learn from previous data, allowing them to identify small deviations from standard transaction patterns that may elude human analysts. Studies by Ashfaq, et al. [24] and Njoku, et al. [39] highlight the efficacy of these models in the early detection of fraud, markedly diminishing financial losses. Through ongoing learning and adaptation to emerging fraud strategies, predictive analytics can identify possible fraud preemptively, enabling financial institutions to respond proactively [40]. This proactive detection is vital, as it minimizes both the economic impact and the reputational damage that can result from fraud.

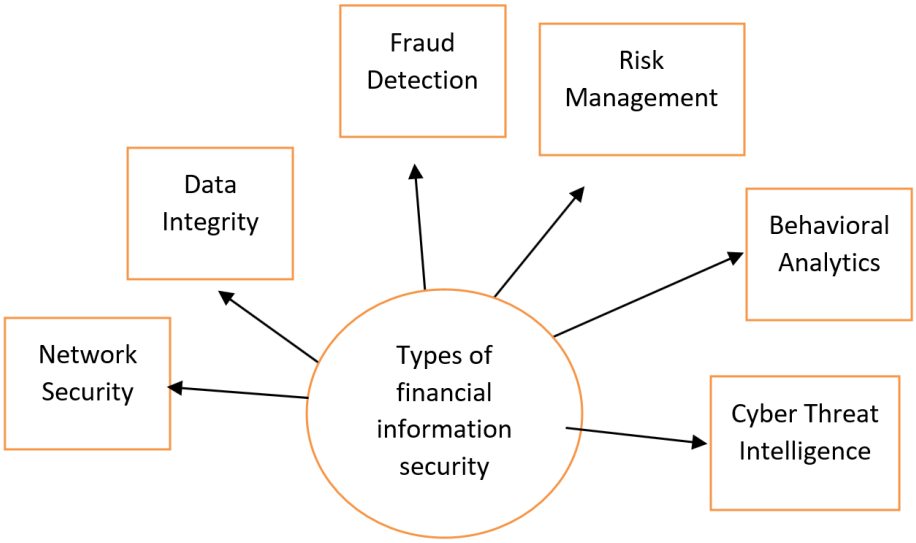

Figure 2.
Categories of financial information security.

However, challenges remain. Predictive models must balance accuracy with compliance to rigorous data privacy legislation, including GDPR and CCPA [12]. Furthermore, models must be robust against adversarial attacks designed to deceive AI systems [14]. Despite these challenges, fraud detection remains a foremost application of Advanced predictive analytics in financial information security significantly contribute to the protection of financial transactions and the maintenance of customer trust.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

4.2. Risk Management in Advanced Predictive Analytics for Financial Information Security

Risk management is a critical function within financial institutions, tasked with identifying, assessing, and mitigating risks that could adversely affect financial assets, operations, or reputation [41]. With the increasing digitization of financial services and the growing sophistication of cyber threats, traditional risk management approaches face significant challenges. Advanced predictive analytics, enhanced by artificial intelligence (AI) and machine learning (ML), provides transformative capabilities. This technology enhances risk management in the realm of financial information security.

AI-driven models can determine subtle approaches and correlations that might go unnoticed through conventional methods [11]. Moreover, AI models facilitate dynamic risk scoring by integrating multiple factors such as market volatility, credit risk, and operational vulnerabilities. This integrated approach supports more holistic and timely decision-making [23]. By using these advanced tools, institutions can optimize their capital reserves, adjust investment strategies, and comply more effectively with regulatory requirements. Despite these benefits, implementing predictive analytics for risk management involves challenges. Data quality and completeness are paramount, Inaccurate or biased data can result in erroneous risk evaluations. Moreover, guaranteeing that predictive models adhere to privacy regulations such as GDPR and CCPA necessitates meticulous design and ongoing oversight [12].

4.3. Behavioral Analytics in Financial Information Security

Behavioural analytics is essential for enhancing financial information security through the utilization of advanced predictive analytics techniques to monitor and analyse user behaviours within financial systems [42]. Unlike traditional security measures that rely heavily on static rules or known threat signatures, behavioral analytics concentrates on comprehending the typical patterns of consumer behavior as well as detecting deviations that may indicate potential fraudulent or malicious actions. This continuous learning process enables the system to establish dynamic behavioral baselines tailored to individual users or groups, which helps in promptly identifying anomalies such as unusual login locations, atypical transaction amounts, or access at unusual times [25]. These anomalies often serve as early warning signs of identity theft, account takeovers, insider threats, or other cyber risks.

The efficacy of behavioral analytics resides in its capacity to identify sophisticated and evolving threats that traditional methods may overlook [43]. For instance, fraudsters may mimic legitimate transaction patterns to avoid detection, but subtle behavioral differences can be captured by predictive models trained to recognize nuanced deviations [44]. However, implementing behavioral analytics also presents challenges, for instance, ensuring data privacy, model precision, and compatibility with outdated systems [12]. The necessity to adhere to legislation such as GDPR and CCPA requires that data collection as well as analysis methods respect user privacy without compromising detection capabilities [45]. Moreover, behavioral models must adapt continuously to evolving user behaviors and emerging cyber threats to maintain effectiveness.

4.4. Cyber Threat Intelligence in Financial Information Security

Cyber Threat Intelligence (CTI) plays a pivotal role in enhancing financial information security, particularly as cyber-attacks become increasingly sophisticated and frequent in the digital age. CTI provides actionable insights within the financial sector by gathering, analyzing, and interpreting information about potential and ongoing cyber threats, as cybercriminals continuously target sensitive data and transactions [46]. This proactive approach aligns closely with the goals of advanced predictive analytics, which aims to identify vulnerabilities and threats before they can cause significant damage.

CTI leverages vast datasets from various sources—including network traffic, threat databases, attack signatures, and dark web monitoring—to identify patterns and emerging threats. When integrated with Artificial Intelligence (AI) and Machine Learning (ML), Cyber Threat Intelligence (CTI) systems may analyze extensive datasets in real time, identifying anomalies or suspicious activities that may signify an imminent threat. This form of analysis allows financial firms to foresee and alleviate hazards more efficiently, transitioning from reactive defense to proactive security management [26, 47].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Moreover, predictive analytics enhances CTI by using historical attack data and threat intelligence feeds to forecast the probability and possible consequences of cyber risks [48]. This forecasting ability allows institutions to prioritize their security resources efficiently, focusing on high-risk threats and adapting their defensive strategies accordingly [49]. For example, machine learning models trained on known attack vectors can detect subtle signals of advanced persistent threats (APTs) or zero-day vulnerabilities that conventional systems may overlook.

However, implementing effective CTI within financial information security poses challenges. The complexity of integrating CTI tools with legacy systems, guaranteeing compliance with data privacy regulations and sustaining the accuracy and timeliness of intelligence data are ongoing concerns [12]. Additionally, adversarial tactics designed to evade detection require continuous improvement of CTI models to remain robust against novel threats [14].

4.5. Discussion on Network Security in Financial Information Security

Network security plays a critical role in safeguarding financial institutions against the growing threat landscape of cyberattacks [50]. With financial institutions increasingly relying on interconnected digital infrastructures, including cloud platforms, mobile banking, and online transaction systems, the attack surface has dramatically expanded. This makes robust network security essential to mitigate illegal access, data breaches, and service interruptions. Conventional network defenses, like firewalls, intrusion detection systems (IDS), and secure communication protocols, are essential yet increasingly enhanced by predictive analytics driven by artificial intelligence (AI) and machine learning (ML) [51]. Predictive analytics improves network security by always monitoring network traffic and user behavior to identify anomalies that may indicate potential threats, such Distributed Denial of Service (DDoS) assaults, ransomware, or advanced persistent threats (APTs).

4.6. Discussion on Data Integrity in Financial Information Security

In the perspective of financial information security, ensuring data integrity is paramount because financial institutions rely heavily on precise and trustworthy data to make pivotal determinations [52]. Organizations must mitigate risks and adhere to regulatory norms. With the increasing digitization of financial services, data is continuously generated, transmitted, and stored across diverse platforms, including cloud environments and blockchain systems. This expansion introduces vulnerabilities where data can be corrupted, tampered with, or altered by unauthorized actors, leading to severe consequences such as financial losses, legal penalties, and erosion of customer trust [30].

Advanced predictive analytics, powered by machine learning (ML) and artificial intelligence (AI), plays a critical role in safeguarding data integrity within financial systems. Predictive models can monitor and analyze transactional data in real-time to detect anomalies that indicate potential breaches or unauthorized data manipulation. By learning from historical patterns, these models can flag inconsistencies or suspicious activities promptly, enabling institutions to take corrective action before errors propagate or fraud occurs [9].

Moreover, encryption and access control mechanisms complement predictive analytics by securing data against unauthorized access and ensuring that only validated modifications are allowed [49]. Blockchain technology, with its immutable ledger framework, augments data integrity by offering transparent and tamper-resistant records of financial transactions [6].

Despite these technological advancements, maintaining data integrity faces challenges such as integrating predictive models with legacy systems, ensuring compliance with privacy regulations, and managing data quality across multiple sources [12, 19]. Addressing these obstacles requires continuous investment in robust data governance frameworks, regular audits, and ongoing development of adaptive predictive models capable of identifying evolving threats to data accuracy.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

4.7. The Role of Predictive Analytics in Financial Security

The contemporary financial landscape demands advanced analytics due to the growing number and complexity of data, which are essential for improved decision-making, risk management, and security [53]. Predictive analytics involves the application of statistical algorithms, machine learning methodologies, and artificial intelligence (AI) to examine historical data and forecast future results. This technology has acquired prominence in the financial sector owing to its capacity to predict market patterns, evaluate potential risks, and enhance financial performance [54].

Traditional risk management models, primarily relying on historical data and linear assumptions, have struggled to keep up with the complexity of today's interconnected financial systems [55]. The limitations of these traditional models were starkly exposed during the 2008 financial crisis, where interconnected risks and systemic vulnerabilities were not adequately captured. This has led to a paradigm shift, with financial institutions increasingly turning to predictive analytics as a transformative tool to improve risk assessment, mitigate potential losses, and make proactive decisions.

5. Predictive Analytics in Financial Risk Management

5.1. Credit Risk and Loan Default Prediction

The most important application of predictive analytics in the financial sector is in managing credit risk. In traditional models, credit assessments largely relied on borrower histories and basic financial data, such as credit scores [56]. While these models provided valuable insights, they were often limited by their reliance on static data, which failed to capture the dynamic nature of borrower behavior.

Predictive models, particularly machine learning algorithms, are capable of processing large datasets, including transactional data, borrower demographics, and even social media activity [57]. These models use this diverse data to create more accurate predictions about the likelihood of loan defaults. For instance, machine learning methodologies such as decision trees and neural networks analyze patterns from past financial behavior to identify accounts that are at a higher risk of default. This real-time prediction helps financial institutions take corrective action before the risk materializes, such as adjusting loan terms or denying loans to high-risk individuals.

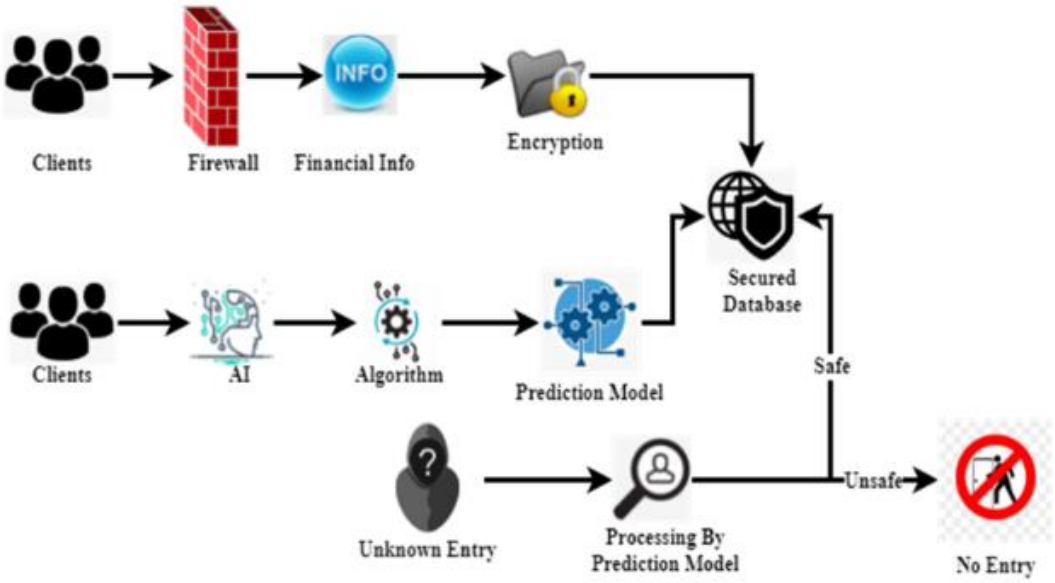

Figure 3.
Cyber Security in Financial Sector Management.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Through the utilization of artificial intelligence, Cyber Security in Financial Sector Management (CS-FSM) does an analysis of all the invasions and provides individuals with the ability to select whether it is safe to participate in Figure 3. A report is sent to the control room or the individuals who are accessing the building if the entry is not stopped.

5.2. Market Risk and Volatility Prediction

Market risk denotes the possibility of financial loss resulting from unfavorable fluctuations in market variables, including stock prices, interest rates, or currency exchange rates [58]. Traditional market risk models, such as Value at Risk (VaR), have limitations, particularly in their inability to incorporate non-linear relationships between variables and to predict the risk in highly volatile markets.

Predictive analytics, on the other hand, uses advanced computational models to forecast potential market movements through the examination of historical data in conjunction with real-time data streams [59]. Methods including time series analysis and ARIMA (Auto Regressive Integrated Moving Average) and machine learning-based models allow financial institutions to predict market volatility and prepare for sudden market shifts. For example, predictive models can identify patterns of volatility that may precede a market crash, enabling firms to adjust their portfolios or hedge their positions proactively.

5.3. Operational Risk and Fraud Detection

Operational risk pertains to the potential for loss arising from insufficient or unsuccessful internal processes, systems, personnel, or external occurrences [60]. Fraud detection is a critical component of operational risk, with predictive analytics serving a fundamental role. Traditional fraud detection models were primarily rule-based, identifying fraudulent transactions based on predefined patterns and criteria [61]. However, these models were often too rigid and unable to detect new forms of fraud or adapt to evolving tactics employed by fraudsters.

Machine learning technologies, like anomaly detection and neural networks, offer a more resilient solution by detecting atypical patterns in transaction data instantaneously. These models may perpetually learn from new data, enabling them to identify potentially fraudulent activities that diverge from established trends. Machine learning algorithms can identify anomalous spending patterns that may suggest credit card fraud or flag dubious transactions in online banking systems. This proactive strategy markedly diminishes revenue losses and fortifies security protocols.

6. Strategic Decision-Making with Predictive Analytics

Predictive analytics not only enhances risk management but also informs strategic decision-making in financial institutions. By forecasting market trends, customer behavior, and economic indicators, predictive models provide valuable insights that guide high-level business decisions [62].

6.1. Financial Forecasting and Budgeting

A crucial use of predictive analytics is financial forecasting. Financial institutions and organizations depend on precise forecasts to strategize their budgets, distribute resources, and control operating expenses [63]. Predictive models utilize previous financial data, economic trends, and market indicators to produce more accurate forecasts, allowing businesses to plan for future growth or mitigate potential losses in case of market downturns.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Figure 4.
Cybersecurity in financial management.
Source: Mishra [64].

Cybersecurity is essential for protecting systems, networks, and technologies against unauthorized access. In the contemporary technological landscape, a corporation must maintain a specialized cybersecurity team to oversee potential cyber-attacks and formulate counterstrategies. Figure 4 illustrates the fundamental components of cybersecurity [64]. Cybersecurity primarily encompasses safe payment systems, user online privacy, antivirus firewalls, mobile security, security locks, data protection, computer protection, and a comprehensive worldwide shield.

6.2. Portfolio Management and Investment Strategies

Predictive analytics has transformed portfolio management by providing insights into prospective investment opportunities and market conditions [65]. Through the analysis of historical performance data, asset correlations, and economic variables, predictive models assist investment managers in optimizing portfolio allocations, thereby enhancing the balance between risk and return.

Machine learning algorithms can evaluate extensive datasets to forecast the performance of different securities in response to fluctuating market conditions. This enables portfolio managers to make more educated investment choices, such as identifying undervalued assets or divesting from overexposed sectors. Predictive analytics also aids in optimizing asset allocations by identifying market trends and aligning them with the institution's risk tolerance and investment goals [66].

7. Challenges in Implementing Predictive Analytics in Financial Information Security

The advantages of predictive analytics in financial security are evident; yet, its implementation presents numerous problems that businesses must confront to properly harness its potential.

7.1. Data Privacy and Security Concerns

Predictive analytics in financial information security entails the aggregation and analysis of extensive sensitive data, encompassing financial transactions, personal details, and behavioral information [67]. Such processing presents considerable privacy and security issues, particularly in light of rigorous legislation like the General Data Protection Regulation (GDPR) in the European Union. To mitigate

these issues, financial organizations must adopt stringent data security protocols, including encryption, safe data storage, and access control systems. Furthermore, predictive models must be constructed to anonymize or de-identify personal data to ensure adherence to privacy requirements while still producing significant insights [68].

7.2. Model Accuracy and Data Quality

The effectiveness of predictive analytics heavily depends on the quality and accuracy of the data used to train the models. Incomplete or erroneous data can lead to inaccurate predictions, potentially resulting in financial losses or misguided business strategies. Financial institutions must invest in data quality management practices, such as data cleaning, validation, and normalization, to ensure that the data used in predictive models is accurate and reliable [69]. Additionally, continuous monitoring and updating of models are essential to adapt to changes in market dynamics and emerging risks.

7.3. Skill Gaps and Integration Challenges

A notable difficulty is the scarcity of proficient professionals qualified to install and manage advanced predictive analytics systems. Financial organizations necessitate data scientists, machine learning professionals, and domain experts capable of constructing, evaluating, and sustaining predictive models [70]. Furthermore, incorporating predictive analytics into current financial systems and workflows can be intricate, particularly for firm's dependent on legacy systems. Institutions must allocate resources for workforce training and infrastructure enhancement to facilitate the seamless incorporation of sophisticated instruments.

8. Sector-Wide Implications and Strategic Recommendations

8.1. Regulatory Compliance and Market Stability

The integration of predictive analytics in financial risk management offers significant sector-wide implications. As financial institutions increasingly depend on data-driven insights to evaluate risks and make choices, the general stability of the financial market enhances. Predictive models can detect nascent dangers promptly, allowing financial institutions to implement remedial measures before these risks develop into systemic threats. Moreover, predictive analytics is essential for maintaining regulatory compliance. By utilizing predictive models to oversee financial transactions and evaluate adherence to regulatory standards, financial organizations can reduce the risk of penalties and reputational harm [71].

8.2. Recommendations for Maximizing Benefits

To maximize the advantages of predictive analytics for financial institutions should adopt a strategic approach that includes the following key recommendations:

1. Invest in Data Security: Implement robust data security frameworks to safeguard confidential information and adhere to privacy standards.
2. Enhance Data Quality: Emphasize data quality management methods to guarantee the precision and dependability of the data utilized in predictive models.
3. Upskill the Workforce: Provide training and development programs to furnish personnel with the requisite competencies to utilize predictive analytics proficiently.
4. Foster Collaboration: Promote collaboration between data scientists, financial analysts, and IT department to guarantee the effective incorporation of predictive models into financial decision-making procedures.

Predictive analytics has proven to be a transformative tool in financial information security, enabling institutions to enhance risk management, improve decision-making, and ensure market stability [72]. By harnessing advanced technologies such as machine learning, big data analytics, and AI, financial institutions can make more accurate predictions, proactively manage risks, and optimize financial outcomes. However, challenges related to data privacy, model accuracy, and workforce skills must be addressed for successful implementation. As the financial landscape continues to evolve, the role of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

predictive analytics will only become more critical in ensuring the resilience and sustainability of financial markets.

8.3. Key Market Trends

- Increasing adoption of AI and ML in advanced analytics solutions: The incorporation of Artificial Intelligence (AI) and Machine Learning (ML) into sophisticated analytics solutions is a significant development. These technologies augment the functionalities of analytics tools, facilitating more precise forecasts and insights.
- Growing demand for real-time analytics: Real-time analytics is increasingly favored as firms aim to make prompt decisions based on the most current data. This trend is especially pertinent in dynamic sectors like banking and e-commerce [73].
- Increasing use of predictive analytics in various industries: Predictive analytics is being adopted across various sectors, including banking and healthcare. Its capacity to predict forthcoming occurrences and patterns is propelling its utilization for strategic decision-making.
- Growing popularity of cloud-based advanced analytics solutions: Cloud-based advanced analytics solutions are gaining popularity for their flexibility, scalability, and accessibility, meeting the expanding requirements of contemporary enterprises.

8.4. Future Trends in Financial Information Security

8.4.1. Artificial Intelligence and Machine Learning for Real-Time Threat Detection

A prominent trend influencing the future of financial information security is the heightened use of Artificial Intelligence (AI) and Machine Learning (ML) for real-time threat identification and prevention [74]. As cyber threats increasingly advance in complexity, conventional security solutions frequently prove insufficient. Artificial Intelligence and Machine Learning, through the analysis of extensive datasets and the identification of user behavior patterns, may identify abnormalities and potential dangers significantly more rapidly than human analysts [75]. This will enable financial institutions to implement preventive strategies to avert cyber-attacks prior to their occurrence [76]. Advanced machine learning models will not only identify known dangers but also anticipate and adjust to novel, previously unrecognised attack techniques, therefore enhancing the security posture of financial systems over time.

8.4.2. Blockchain Technology for Enhanced Data Integrity and Security

A burgeoning trend is the incorporation of blockchain technology in the security of financial information. The decentralised nature of blockchain guarantees data security, transparency, and immutability. In financial systems, these features could revolutionise processes such as transaction verification, secure payment systems, and contract execution. By providing a tamper-proof ledger, blockchain can help reduce fraud and enhance data integrity. Additionally, blockchain could be used to track and authenticate financial transactions, ensuring that all data remains secure, even in a highly connected digital world [77].

8.4.3. Cloud Security Innovations and Hybrid Security Models

As financial institutions increasingly migrate to cloud-based environments, securing these platforms will become a priority. The rise of cloud computing has led to more agile, scalable systems, but it also introduces unique security challenges. Future trends will see the development of more cloud-specific security frameworks, offering robust protection for sensitive financial data stored in cloud environments [78]. Additionally, hybrid security models, combining both on-premise and cloud solutions, will likely become more prevalent to ensure comprehensive data protection. Financial institutions will focus on securing data across multiple platforms while ensuring regulatory compliance and privacy standards.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

8.4.4. Privacy-Preserving Technologies and Regulations

As worries regarding data privacy escalate, particularly due to rigorous rules such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), the future of financial information security will progressively emphasize privacy-preserving solutions. Differential Privacy and Federated Learning are two emerging technologies enabling financial institutions to analyze data while safeguarding individual privacy [79]. These strategies facilitate the training of prediction models using aggregated data while safeguarding sensitive information from exposure., which would be particularly important in areas such as customer behavior analysis and fraud detection [80].

8.4.5. Quantum Computing and Post-Quantum Cryptography

Quantum computing is expected to revolutionise many industries, including financial information security. While it is still in the initial phases, quantum computing holds the promise of disrupting numerous cryptographic systems that currently protect financial transactions [81]. In response, post-quantum cryptography is being developed to create encryption algorithms resistant to quantum attacks [82]. Financial institutions will need to stay ahead of these advancements by implementing quantum-safe cryptographic protocols to safeguard sensitive financial data in the coming years.

9. Advanced Threat Intelligence and Predictive Analytics

The future of financial information security will also see the evolution of advanced threat intelligence tools, powered by AI and big data analytics. These tools will consistently monitor and evaluate security data from diverse sources, delivering immediate insights on developing threats. The integration of predictive analytics with threat intelligence empowers financial institutions to foresee and address risks proactively, before they emerge [83]. By leveraging data from historical cyber-attacks, financial organizations will be able to predict the likelihood of new threats and adapt their security strategies accordingly. One of the greatest predictive analytics methods is decision trees since it can handle missing variables and is easy to understand. To visually represent the alternatives arising from each choice or outcome, decision trees employ branching [39]. Three different regression approaches are available for various contexts.

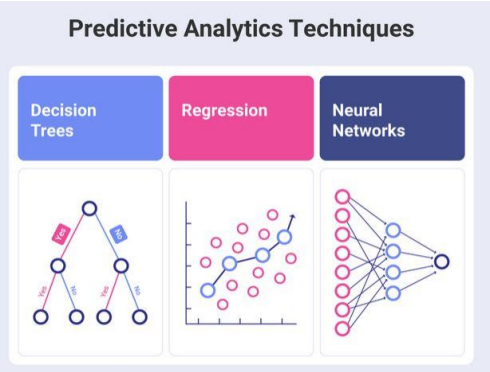

Figure 5.
Types of Predictive Analytics.

Regression can be applied differently depending on the data query, but in general, the predictive analytics regression technique helps to understand the correlations between variables in figure 5. When an outcome can be attributed to only one independent variable, linear regression is employed. If an outcome is influenced by more than one independent variable, multiple regression is employed. Additionally, when the dependent variable is binary, logistic regression is employed [82]. The most complex predictive analytics method is neural networks. It makes use of algorithms to identify potential connections among data sets in Figure 5. By using AI, neural networks enable more complex pattern

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

identification. In order to draw conclusions about the data it meets, predictive analytics mostly depends on intricate models and algorithms. In order to forecast future trends, these predictive analytics approaches analyse both historical and present data using algorithms and machine learning [81]. Neural networks, regression, and decision trees are the three primary methods in predictive analytics.

10. Security Automation and Orchestration

To combat the growing volume and complexity of cyber threats, financial institutions will increasingly implement security automation and orchestration technologies. These solutions will help automate routine security tasks such as incident response, threat detection, and vulnerability management [84]. With AI-driven automation, security teams can focus on more complex issues, while automated systems handle repetitive tasks, reducing response times and minimizing human error [85].

Table 3.
Overview of Financial Information Security Categories, Applications, and Implications.

Types of Financial Information Security	Prospective Applications	Method	Key Findings	Implications	Source
Fraud Detection	Machine learning models detect peculiar transaction patterns to prevent real-time fraud. Models learn from historical data to improve accuracy.	Systematic reviews, ML model analysis	Predictive models can detect fraud early, reducing losses.	Enhanced real-time fraud prevention and financial security.	Ashfaq, et al. [24] and Njoku, et al. [39]
Risk Management	AI-based models assess risks in transactions, investments, or customers by analyzing behavior and trends.	AI and ML model application, review	AI models help in continuous risk monitoring and alerting.	Better informed decisions and risk mitigation.	Williams, et al. [11] and Fritz-Morgenthal, et al. [23]
Behavioral Analytics	Predictive analytics monitors user behavior to detect anomalies like unusual logins or transactions.	Behavioral data analysis, ML algorithms	Early detection of identity theft and account takeovers.	Reduced unauthorized access and fraud risk.	Shah, et al. [25] and Abbasi, et al. [44]
Cyber Threat Intelligence	AI models predict cyber-attacks by analyzing network traffic, attack history, and threat feeds.	Cybersecurity data analysis, AI models	AI can preemptively identify and mitigate cyber threats.	Proactive cybersecurity management in financial institutions.	Yeboah-Ofori, et al. [26] and Bala and Behal [47]
Encryption	Protect sensitive financial data by converting into unreadable formats during transmission/storage.	Cryptography implementation and review	Encryption ensures data privacy and confidentiality.	Secure transmission and storage of financial information.	Karbasi and Shahpasand [27]
Access Control	Ensure only authorized personnel access sensitive financial data, preventing breaches.	Security policy reviews, access management	Access control reduces unauthorized data access.	Improved internal security and data protection.	Ward and Smith [28]
Network Security	Firewalls, intrusion detection systems, and secure protocols serve to thwart unauthorised network access and mitigate cyber-attacks.	Network security frameworks and evaluations	Robust network security reduces risk of cyber intrusion.	Strengthened defense against external cyber threats.	Qasaimeh, et al. [29]
Data Integrity	Ensure data accuracy, consistency, and reliability by detecting and preventing unauthorised alterations.	Data audit and integrity protocols	Regular audits maintain trustworthy financial data.	Trustworthy financial records and compliance assurance.	Sabale, et al. [30]

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

10.1. Implications of the Study

The integration of advanced predictive analytics in financial information security carries serious consequences for both the financial industry and the broader cybersecurity landscape. This study underscores how predictive analytics, using machine learning and artificial intelligence, can transform the way financial institutions identify, mitigate, and respond to emerging cyber threats [86].

10.2. Practical Implications

Financial institutions might utilise the findings to create more proactive and dynamic security systems that are capable of detecting and preventing threats in real-time. By adopting predictive models, organizations can switch from reactive defence mechanisms to anticipatory strategies, thereby reducing the frequency and impact of cyberattacks [73]. Enhanced fraud detection capabilities and risk assessment models have the potential to generate significant cost reductions by minimising losses due to fraudulent transactions and improving credit risk evaluations [87]. Moreover, Enhanced data integrity and privacy-preserving analytics facilitate adherence to rigorous regulatory frameworks like GDPR and CCPA, thereby minimising the potential for legal repercussions and harm to reputation [88].

10.3. Technological Implications

The study emphasises that there must be ongoing innovation in AI and ML algorithms to improve their robustness against adversarial attacks and adjust to the swiftly changing landscape of cyber threats [89]. Financial institutions are encouraged to invest in integrating these predictive analytics tools with their existing legacy systems to maximise their utility and operational effectiveness. Furthermore, the exploration of emerging technologies such as blockchain, quantum-safe cryptography, and security automation offers a pathway toward building more resilient and secure financial infrastructures [90].

10.4. Policy and Regulatory Implications

Findings emphasise the critical role of data privacy and regulatory compliance in the deployment of predictive analytics solutions. Policymakers and regulators can use insights from this study to formulate guidelines that balance innovation in financial cybersecurity with the protection of individual privacy rights [49]. This includes encouraging transparency and explainability in AI-driven decision-making, fostering trust between consumers, financial institutions, and regulatory bodies [91].

10.5. Academic and Research Implications

The study identifies key research gaps, such as the need for models that predict novel cyber-attacks and seamless integration with legacy systems [92]. It calls for further interdisciplinary research combining cybersecurity, finance, data science, and legal expertise to develop holistic and effective predictive frameworks. Future research can build on this foundation to refine methodologies, address ethical concerns, and enhance model interpretability.

In conclusion, the implications of this study highlight that advanced predictive analytics is pivotal for the evolution of financial information security, enabling smarter, faster, and more reliable protection mechanisms [93]. This transformation is essential to sustaining trust and stability in the increasingly digital financial ecosystem.

11. Limitations

Despite the promising capabilities of advanced predictive analytics in enhancing financial information security, this study faces several limitations. Firstly, incorporating predictive models into existing financial systems presents a significant challenge [94].

Numerous financial institutions function using obsolete infrastructures that lack compatibility with modern AI and machine learning technologies, making seamless adoption difficult and costly. Secondly, data privacy and regulatory compliance impose constraints on the extent to which personal and transactional data can be used for model training as well as real-time analytics [95].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

Strict regulations, for example, GDPR and CCPA, require careful balancing of predictive accuracy with privacy protection, limiting data accessibility and potentially impacting model performance. Additionally, Predictive models face significant risks from adversarial attacks, as malicious individuals intentionally alter inputs to mislead systems, raising concerns about model robustness and trustworthiness. Lastly, the scarcity of skilled personnel proficient in both finance and advanced analytics hampers the effective development, deployment, and maintenance of these technologies in many organizations [15].

12. Future Directions

Future investigations should concentrate on creating more flexible and resilient predictive analytics models that can seamlessly integrate with various and legacy financial systems without compromising performance or security [72].

Emphasis should be placed on enhancing model explainability to ensure transparency, regulatory compliance, and greater stakeholder trust. Privacy-preserving machine learning Methods like federated learning and differential privacy present exciting opportunities for enhancing predictive analytics, all while adhering to data protection regulations and ethical standards. Additionally, ongoing work is needed to defend predictive models against adversarial attacks and improve their resilience to evolving cyber threats.

Expanding interdisciplinary training programs will also be critical to bridge the skills gap, equipping financial professionals with expertise in both cybersecurity and data science.

Finally, exploring the integration of emerging technologies like quantum computing and blockchain could further revolutionize predictive capabilities and data security in financial systems.

13. Conclusion

This study highlights the essential function of predictive models in improving real-time threat detection, risk evaluation, and decision-making in the ever-evolving and data-centric financial landscape [83]. Despite the significant benefits, challenges such as data privacy concerns, integration with legacy systems, model robustness against adversarial attacks, and skill shortages remain substantial barriers to widespread adoption. Addressing these limitations requires ongoing innovation in privacy-preserving techniques, improved model transparency, and resilient cybersecurity frameworks [73].

Furthermore, the evolving landscape of cyber threats demands that predictive analytics evolve continuously, incorporating new methodologies and novel technologies like quantum computing and blockchain to uphold robust defence strategies [96].

As financial institutions embrace these advanced analytics tools, they must also invest in workforce development and cross-disciplinary collaboration to fully harness their potential. Ultimately, the successful implementation of predictive analytics will not only strengthen financial information security but also contribute to greater market stability and regulatory compliance, safeguarding both institutions and consumers in a rapidly digitizing financial world.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

References

[1] Z. Zong and Y. Guan, "AI-driven intelligent data analytics and predictive analysis in industry 4.0: Transforming knowledge, innovation, and efficiency," *Journal of the Knowledge Economy*, vol. 16, no. 1, pp. 864-903, 2025/03/01 2025. https://doi.org/10.1007/s13132-024-02001-z

[2] H. A. Javaid, "Ai-driven predictive analytics in finance: Transforming risk assessment and decision-making," *Advances in Computer Sciences*, vol. 7, no. 1, pp. 1-9, 2024.

[3] P. Ghose, M. R. I. Bhuiyan, M. N. Hasan, S. H. Rakib, and L. Mani, "Mediated and moderating variables between behavioral intentions and actual usages of fintech in the USA and Bangladesh through the extended UTAUT model," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 2, pp. 113-125, 2025.

[4] M. A. Al Mahmud *et al.*, "Securing financial information in the digital age: An overview of cybersecurity threat evaluation in banking systems," *Journal of Ecohumanism*, vol. 4, no. 2, pp. 1508 – 1517, 2025. https://doi.org/10.62754/joe.v4i2.6526

[5] A. Despotović, A. Parmaković, and M. Miljković, *Cybercrime and cyber security in fintech in digital transformation of the financial industry: Approaches and applications*. Cham: Springer International Publishing, 2023.

[6] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499-507, 2018. https://doi.org/10.1016/j.scs.2018.02.039

[7] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutionsb," *Electronics*, vol. 12, no. 6, p. 1333, 2023. https://doi.org/10.3390/electronics12061333

[8] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks," *Results in Engineering*, vol. 23, p. 102647, 2024. https://doi.org/10.1016/j.rineng.2024.102647

[9] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects," *Annals of Data Science*, vol. 10, no. 6, pp. 1473-1498, 2023. https://doi.org/10.1007/s40745-022-00444-2

[10] V. Mahalakshmi, N. Kulkarni, K. V. Pradeep Kumar, K. Suresh Kumar, D. Nidhi Sree, and S. Durga, "The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence," *Materials Today: Proceedings*, vol. 56, pp. 2252-2255, 2022. https://doi.org/10.1016/j.matpr.2021.11.577

[11] M. Williams, M. F. Yussuf, and A. O. Olukoya, "Machine learning for proactive cybersecurity risk analysis and fraud prevention in digital finance ecosystems," *Ecosystems*, vol. 20, p. 21, 2021.

[12] B. Munir, M. Irfan, and N. Bashir, "Artificial intelligence, data protection and transparency: A comparative study of GDPR and CCPA," *Artificial Intelligence, Data Protection and Transparency: A Comparative Study of GDPR and CCPA (September 30, 2024)*, 2024.

[13] P. Ghose *et al.*, "The role of financial technology and financial inclusion in sustainable governance and performance: A systematic review of global insights," *Journal of Governance & Regulation*, vol. 14, no. 2, pp. 341–352, 2025. https://doi.org/10.22495/jgrv14i2siart13

[14] H. Baniecki and P. Biecek, "Adversarial attacks and defenses in explainable artificial intelligence: A survey," *Information Fusion*, vol. 107, p. 102303, 2024. https://doi.org/10.1016/j.inffus.2024.102303

[15] J. M. Nwaogu, Y. Yang, A. P. C. Chan, and X. Wang, "Enhancing drone operator competency within the construction industry: Assessing training needs and roadmap for skill development," *Buildings*, vol. 14, no. 4, p. 1153, 2024. https://doi.org/10.3390/buildings14041153

[16] F. Ekundayo, I. Atoyebi, A. Soyele, and E. Ogunwobi, "Predictive analytics for cyber threat intelligence in fintech using big data and machine learning," *International Journal of Research and Publications Review*, vol. 5, no. 11, pp. 1-15, 2024.

[17] A. Aljohani, "Predictive analytics and machine learning for real-time supply chain risk mitigation and agility," *Sustainability*, vol. 15, no. 20, p. 15088, 2023. https://doi.org/10.3390/su152015088

[18] M. M. Maja and P. Letaba, "Towards a data-driven technology roadmap for the bank of the future: Exploring big data analytics to support technology roadmapping," *Social Sciences & Humanities Open*, vol. 6, no. 1, p. 100270, 2022. https://doi.org/10.1016/j.ssaho.2022.100270

[19] M. M. Rahman, B. P. Pokharel, S. A. Sayeed, S. K. Bhowmik, N. Kshetri, and N. Eashrak, "riskAIchain: AI-driven IT infrastructure—blockchain-backed approach for enhanced risk management," *Risks*, vol. 12, no. 12, p. 206, 2024. https://doi.org/10.3390/risks12120206

[20] W. Steingartner, D. Galinec, and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," *Symmetry*, vol. 13, no. 4, p. 597, 2021. https://doi.org/10.3390/sym13040597

[21] P. Ghose, M. Parvin, S. Akter, S. H. Rakib, and M. R. Islam, "Gravitating towards technology-based emerging financial crime: A PRISMA-based systematic," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 2, p. 2025, 2025.

[22] A. A. H. de Hond *et al.*, "Guidelines and quality criteria for artificial intelligence-based prediction models in healthcare: A scoping review," *NPJ Digital Medicine*, vol. 5, no. 1, p. 2, 2022. https://doi.org/10.1038/s41746-021-00549-7

[23] S. Fritz-Morgenthal, B. Hein, and J. Papenbrock, "Financial risk management and explainable, trustworthy, responsible AI," *Frontiers in Artificial Intelligence*, vol. 5, p. 779799, 2022. https://doi.org/10.3389/frai.2022.779799

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

[24] T. Ashfaq *et al.*, "A machine learning and blockchain based efficient fraud detection mechanism," *Sensors*, vol. 22, no. 19, p. 7162, 2022. https://doi.org/10.3390/s22197162

[25] S. Shah *et al.*, "Compromised user credentials detection in a digital enterprise using behavioral analytics," *Future Generation Computer Systems*, vol. 93, pp. 407-417, 2019. https://doi.org/10.1016/j.future.2018.09.064

[26] A. Yeboah-Ofori *et al.*, "Cyber threat predictive analytics for improving cyber supply chain security," *IEEE Access*, vol. 9, pp. 94318-94337, 2021. https://doi.org/10.1109/ACCESS.2021.3087109

[27] A. H. Karbasi and S. Shahpasand, "A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1423-1441, 2020. https://doi.org/10.1007/s12083-020-00901-w

[28] P. Ward and C. L. Smith, "The development of access control policies for information technology systems," *Computers & Security*, vol. 21, no. 4, pp. 356-371, 2002. https://doi.org/10.1016/S0167-4048(02)00414-5

[29] M. Qasaimeh, R. A. Hammour, M. B. Yassein, R. S. Al-Qassas, J. A. L. Torralbo, and D. Lizcano, "Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions," *Journal of Software: Evolution and Process*, vol. 34, no. 11, p. e2489, 2022. https://doi.org/10.1002/smr.2489

[30] M. M. Sabale, V. A. Pande, A. A. Tagalpallewar, A. G. Swami, A. T. Pawar, and A. M. Baheti, "Maintaining data safety and accuracy through data integrity (DI): A comprehensive review," *Research Journal of Pharmacy and Technology*, vol. 17, no. 5, pp. 2431-2440, 2024. http://dx.doi.org/10.52711/0974-360X.2024.00381

[31] A. Mimi and L. Mani, "Gravitating the gig economy for reshaping the careers using technological platform in the digital age in an emerging economy," *Journal of Information Systems and Informatics*, vol. 6, no. 4, pp. 3129-3161, 2024.

[32] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021.

[33] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and The PRISMA Group, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Medicine*, vol. 6, no. 7, p. e1000097, 2009.

[34] T. Pervin *et al.*, "A Hybrid CNN-LSTM approach for detecting anomalous bank transactions: Enhancing financial fraud detection accuracy," *The American Journal of Management and Economics Innovations*, vol. 7, no. 04, pp. 116-123, 2025.

[35] M. I. Bhuiyan, M. N. U. Milon, R. Hossain, T. A. Poli, and M. A. Salam, "Examining the relationship between poverty and juvenile delinquency trends in a developing country," *Academic Journal of Interdisciplinary Studies*, vol. 13, no. 6, pp. 255-274, 2024.

[36] R. Malhotra and D. Malhotra, "The impact of technology, big data, and analytics: The evolving data-driven model of innovation in the finance industry," *Journal of Financial Data Science*, vol. 5, no. 3, p. 129, 2023. https://doi.org/10.3905/jfds.2023.1.129

[37] L. Mani, "Gravitating towards the digital economy: Opportunities and challenges for transforming smart Bangladesh," *Pakistan Journal of Life & Social Sciences*, vol. 22, no. 1, pp. 3324–3334, 2024.

[38] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, p. 116429, 2022. https://doi.org/10.1016/j.eswa.2021.116429

[39] D. O. Njoku, V. C. Iwuchukwu, J. E. Jibiri, C. T. Ikwuazom, C. I. Ofoegbu, and F. O. Nwokoma, "Machine learning approach for fraud detection system in financial institution: A web base application," *Machine Learning*, vol. 20, no. 4, pp. 1–12, 2024.

[40] M. I. Pramanik, P. Ghose, M. Hossen, M. Ahmed, M. Rahman, and M. Bhuiyan, "Emerging technological trends in financial crime and money laundering: A bibliometric analysis of cryptocurrency's role and global research collaboration," *Journal of Posthumanism*, vol. 5, no. 6, pp. 3611–3633, 2025.

[41] S. Pakhchanyan, "Operational risk management in financial institutions: A literature review," *International Journal of Financial Studies*, vol. 4, no. 4, p. 20, 2016. https://doi.org/10.3390/ijfs4040020

[42] M. Arunkumar, K. Rajkumar, W. Jeyaseelan, and N. Natraj, "Data mining, machine learning, and statistical modeling for predictive analytics with behavioral big data," *Tehnički vjesnik*, vol. 32, no. 1, pp. 72-77, 2025. https://doi.org/10.17559/TV-20231102001073

[43] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907-30927, 2024. https://doi.org/10.1109/ACCESS.2024.3369906

[44] A. Abbasi, R. Y. Lau, and D. E. Brown, "Predicting behavior," *IEEE Intelligent Systems*, vol. 30, no. 3, pp. 35-43, 2015. https://doi.org/10.1109/MIS.2015.19

[45] M. Khatun, R. Islam, S. Kumar, R. Hossain, and L. Mani, "The impact of artificial intelligence on educational transformation: Trends and future directions," *Journal of Information Systems and Informatics*, vol. 6, no. 4, pp. 2347-2373, 2024.

[46] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023. https://doi.org/10.3390/s23167273.

[47] B. Bala and S. Behal, "AI techniques for Iot-based DDoS attack detection: Taxonomies, comprehensive review and research challenges," *Computer Science Review*, vol. 52, p. 100631, 2024. https://doi.org/10.1016/j.cosrev.2024.100631

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

[48] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Computers & Security*, vol. 67, pp. 35-58, 2017. https://doi.org/10.1016/j.cose.2017.02.005

[49] M. R. I. Bhuiyan, "Industry readiness and adaptation of fourth industrial revolution: Applying the extended TOE framework," *Human Behavior and Emerging Technologies*, vol. 2024, no. 1, p. 8830228, 2024.

[50] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz013, 2019.

[51] S. U. Khan, F. Eusufzai, M. Azharuddin Redwan, M. Ahmed, and S. R. Sabuj, "Artificialintelligence for cyber security: Performance analysis of network intrusion detection," in *Explainable Artificial Intelligence for Cyber Security: Next Generation Artificial Intelligence*, M. Ahmed, S. R. Islam, A. Anwar, N. Moustafa, and A.-S. K. Pathan Eds. Cham: Springer International Publishing, 2022.

[52] S. V. Flowerday and R. Von Solms, "Real-time information integrity = real-time business integrity," *Computers & Security*, vol. 24, no. 8, pp. 604–613, 2005.

[53] S.-A. Ionescu and V. Diaconita, "Transforming financial decision-making: The interplay of AI, cloud computing and advanced data management technologies," *International Journal of Computers Communications & Control*, vol. 18, no. 6, 2023.

[54] M. A. J. Riaj, M. N. Tabassum, R. Hossain, M. R. I. Bhuiyan, and M. Khatun, "Digitalization transformation in entrepreneurship and enterprise green innovation," in *Digitizing Green Entrepreneurship*: IGI Global Scientific Publishing, 2025.

[55] O. Renn, K. Lucas, A. Haas, and C. Jaeger, "Things are different today: The challenge of global systemic risks," *Journal of Risk Research*, vol. 22, no. 4, pp. 401-415, 2019. https://doi.org/10.1080/13669877.2017.1409252

[56] B. W. Yap, S. H. Ong, and N. H. M. Husain, "Using data mining to improve assessment of credit worthiness via credit scoring models," *Expert Systems with Applications*, vol. 38, no. 10, pp. 13274-13283, 2011. https://doi.org/10.1016/j.eswa.2011.04.147

[57] A. E. Khandani, A. J. Kim, and A. W. Lo, "Consumer credit-risk models via machine-learning algorithms," *Journal of Banking & Finance*, vol. 34, no. 11, pp. 2767-2787, 2010. https://doi.org/10.1016/j.jbankfin.2010.06.001

[58] E. L. Grinols and S. J. Turnovsky, "Risk, the financial market, and macroeconomic equilibrium," *Journal of Economic Dynamics and Control*, vol. 17, no. 1, pp. 1-36, 1993. https://doi.org/10.1016/S0165-1889(06)80002-3

[59] R. Iqbal, F. Doctor, B. More, S. Mahmud, and U. Yousuf, "Big data analytics: Computational intelligence techniques and application areas," *Technological Forecasting and Social Change*, vol. 153, p. 119253, 2020.

[60] M. A. Lewis, "Cause, consequence and control: Towards a theoretical and practical model of operational risk," *Journal of Operations Management*, vol. 21, no. 2, pp. 205-224, 2003. https://doi.org/10.1016/S0272-6963(02)00071-2

[61] J. Kim, H. Jung, and W. Kim, "Sequential pattern mining approach for personalized fraudulent transaction detection in online banking," *Sustainability*, vol. 14, no. 15, p. 9791, 2022. https://doi.org/10.3390/su14159791

[62] R. Kasemrat, T. Kraiwanit, and N. Yuenyong, "Predictive analytics in customer behavior: unveiling economic and governance insights through machine learning," *Journal of Governance and Regulation/Volume*, vol. 14, no. 1, 2025. https://doi.org/10.22495/jgrv14i1siart8

[63] K. O. Prakash, K. A. Abdullah, R. Daoud, Y. Moulana, and M. T. Matriano, "The budgeting and forecasting analysis and the impact on company financial performance and strategic decision-making: A case of national finance, Oman," *Gsj*, vol. 12, no. 6, pp. 2133-2157, 2024.

[64] S. Mishra, "Exploring the impact of AI-based cyber security financial sector management," *Applied Sciences*, vol. 13, no. 10, p. 5875, 2023. https://doi.org/10.3390/app13105875

[65] S. Kumar, D. Sharma, S. Rao, W. M. Lim, and S. K. Mangla, "Past, present, and future of sustainable finance: Insights from big data analytics through machine learning of scholarly research," *Annals of Operations Research*, vol. 345, no. 2, pp. 1061-1104, 2025. https://doi.org/10.1007/s10479-021-04410-8

[66] S. Lyu and Z. Jiao, "Optimization of financial asset allocation and risk management strategies combining internet of things and clustering algorithms," *IEEE Internet of Things Journal*, vol. 12, no. 4, pp. 3654-3669, 2025. https://doi.org/10.1109/JIOT.2024.3486714

[67] T. K. Vashishth, V. Sharma, B. Kumar, and K. K. Sharma, "Cloud-based data management for behavior analytics in business and finance sectors," in *Data-Driven Modelling and Predictive Analytics in Business and Finance*: Auerbach Publications, 2024.

[68] S. Sampaio, P. R. Sousa, C. Martins, A. Ferreira, L. Antunes, and R. Cruz-Correia, "Collecting, processing and secondary using personal and (pseudo)anonymized data in smart cities," *Applied Sciences*, vol. 13, no. 6, p. 3830, 2023. https://doi.org/10.3390/app13063830

[69] W. Elouataoui, S. El Mendili, and Y. Gahi, "An automated big data quality anomaly correction framework using predictive analysis," *Data*, vol. 8, no. 12, p. 182, 2023. https://doi.org/10.3390/data8120182

[70] R. Elshawi, S. Sakr, D. Talia, and P. Trunfio, "Big data systems meet machine learning challenges: Towards big data science as a service," *Big Data Research*, vol. 14, pp. 1-11, 2018. https://doi.org/10.1016/j.bdr.2018.04.004

[71] M. S. A. Lee, L. Floridi, and A. Denev, "Innovating with confidence: Embedding ai governance and fairness in a financial services risk management framework." Cham: Springer International Publishing, 2021.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

[72] H. Allioui and Y. Mourdi, "Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey," *Sensors*, vol. 23, no. 19, p. 8015, 2023. https://doi.org/10.3390/s23198015
[73] M. R. I. Bhuiyan, M. R. Faraji, M. Rashid, M. Bhuyan, R. Hossain, and P. Ghose, "Digital transformation in SMEs emerging technological tools and technologies for enhancing the SME's strategies and outcomes," *Journal of Ecohumanism*, vol. 3, no. 4, pp. 211-224, 2024. https://doi.org/10.62754/joe.v3i4.3594
[74] M. El Hajj and J. Hammoud, "Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of ai applications in trading, risk management, and financial operations," *Journal of Risk and Financial Management*, vol. 16, no. 10, p. 434, 2023. https://doi.org/10.3390/jrfm16100434
[75] A. G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: Current models and applications," *Applied Intelligence*, vol. 51, no. 8, pp. 6029-6055, 2021. https://doi.org/10.1007/s10489-020-02160-x
[76] M. R. I. Bhuiyan, T. Husain, S. Islam, and A. Amin, "Exploring the prospective influence of artificial intelligence on the health sector in Bangladesh: a study on awareness, perception and adoption," *Health Education*, vol. 125, no. 3, pp. 279-297, 2025.
[77] S. Ahamad, P. Gupta, P. Bikash Acharjee, K. Padma Kiran, Z. Khan, and M. Faez Hasan, "The role of block chain technology and internet of things (IoT) to protect financial transactions in crypto currency market," *Materials Today: Proceedings*, vol. 56, pp. 2070-2074, 2022. https://doi.org/10.1016/j.matpr.2021.11.405
[78] S. Drissi, M. Chergui, and Z. Khatar, "A systematic literature review on risk assessment in cloud computing: Recent research advancements," *IEEE Access*, vol. 13, pp. 76289-76307, 2025. https://doi.org/10.1109/ACCESS.2025.3561123
[79] M. Yuxin and W. Honglin, "Federated learning based on data divergence and differential privacy in financial risk control research," *Computers, Materials and Continua*, vol. 75, no. 1, pp. 863-878, 2023. https://doi.org/10.32604/cmc.2023.034879
[80] A. Amin, M. R. I. Bhuiyan, R. Hossain, C. Molla, T. A. Poli, and M. N. U. Milon, "The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country," *Business Strategy & Development*, vol. 7, no. 2, p. e363, 2024. https://doi.org/10.1002/bsd2.363
[81] N. R. Mosteanu and A. Faccia, "Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 1, p. 19, 2021. https://doi.org/10.3390/joitmc7010019
[82] M. A. Islam and M. R. I. Bhuiyan, "Digital transformation and society," Rochester, NY, 2022.
[83] A. Abisoye and J. I. Akerele, "High-impact data-driven decision-making model for integrating cutting-edge cybersecurity strategies into public policy," *Governance, and Organizational Frameworks*, 2021.
[84] M. Papel, A. Mridha, A. Rahman, and M. Ashrafuzzaman, "Enhancing government it infrastructure: Develop frameworks for modernizing government it systems to improve security, efficiency, and citizen engagement," *Frontiers in Applied Engineering and Technology*, vol. 1, no. 01, pp. 157-174, 2024.
[85] A. Tariq *et al.*, "Optimizing optical, dielectric, structural, and electrical properties in cu-substituted Mg-Zn ferrite nanoparticles: Insights for sustainable energy and environmental solutions," *Journal of Alloys and Compounds*, p. 182252, 2025.
[86] K. C. Nwafor, A. O. Ikudabo, and C. C. Onyeje, "Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics," *International Journal of Scientific Research and Applications*, 2024. https://doi.org/10.30574/ijsra.2024.13.1.2014
[87] N. Akter *et al.*, "Advanced detection and forecasting of fake news on social media platforms using natural language processing and artificial intelligence," *Journal of Posthumanism*, vol. 5, no. 6, pp. 3208-3236, 2025.
[88] A. K. Y. Yanamala and S. Suryadevara, "Navigating data protection challenges in the era of artificial intelligence: A comprehensive review," *Revista de Inteligencia Artificial en Medicina*, vol. 15, no. 1, pp. 113-146, 2024.
[89] M. I. Hossain, T. Sultana, M. N. U. Islam, A. Akther, A. F. Sarpong, and F. Akter, "Enhancing project management through outsourcing: Transforming growth in information technology (it)," *Journal of Knowledge Management Practice*, vol. 25, no. 1, 2025. https://doi.org/10.62477/jkmp.v25i1.489
[90] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Computers & Security*, vol. 142, p. 103883, 2024. https://doi.org/10.1016/j.cose.2024.103883
[91] E. E. Agu, A. O. Abhulimen, A. N. Obiki-Osafiele, O. S. Osundare, I. A. Adeniran, and C. P. Efunniyi, "Discussing ethical considerations and solutions for ensuring fairness in AI-driven financial services," *International Journal of Frontier Research in Science*, vol. 3, no. 2, pp. 001-009, 2024. https://doi.org/10.56355/ijfrms.2024.3.2.0024
[92] J. Yu, A. V. Shvetsov, and A. S. Hamood, "Leveraging machine learning for cybersecurity resilience in industry 4.0: Challenges and future directions," *IEEE Access*, vol. 12, pp. 159579-159596, 2024. https://doi.org/10.1109/ACCESS.2024.3482987

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
DOI: 10.55214/2576-8484.v9i7.9142

[93] A. A. Sunna, T. Sultana, N. Kshetri, and M. M. Uddin, "AssessCICA: Assessing and mitigating financial losses from cyber attacks with role of cyber insurance in post-pandemic era," presented at the In 2025 13th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE, 2025.
[94] D. Broby, "The use of predictive analytics in finance," *The Journal of Finance and Data Science*, vol. 8, pp. 145-161, 2022. https://doi.org/10.1016/j.jfds.2022.05.003
[95] J. Wieringa, P. K. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera, "Data analytics in a privacy-concerned world," *Journal of Business Research*, vol. 122, pp. 915-925, 2021. https://doi.org/10.1016/j.jbusres.2019.05.005
[96] D. Chatziamanetoglou and K. Rantos, "Cyber threat intelligence on blockchain: A systematic literature review," *Computers*, vol. 13, no. 3, p. 60, 2024. https://doi.org/10.3390/computers13030060

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 7: 2222-2245, 2025
***DOI:** 10.55214/2576-8484.v9i7.9142*