Journal of Global Research in Electronics and Communication
Volume 2, No. 2, February 2026
Available Online at: www.jgrec.info

REVIEW PAPER

Forecasting Cyber Attacks in Banking and FinTech Platforms: A Review of Data-Driven Approaches

Mr. Himanshu Barhaiya
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Bhopal
himanshub@lnct.ac.in

***Abstract*— It is essential to predict cyber-attacks in financial systems and FinTech platforms to protect financial infrastructures with an ever-advancing threat level. The review will discuss evidence-based solutions that improve the predictive abilities of the Security Information and Event Management (SIEM). Through systematic study of machine learning, deep learning, and statistical models on historical security event data, it identifies key methods for predicting attack vectors such as phishing, DDoS, fraud, and malware infiltration. The exploratory paper identifies feature engineering, anomaly detection, and real-time analytics as components that enhance the accuracy of forecasting. Issues such as imbalanced data, concept drift and latency in large-scale environments are addressed, and new methods such as ensemble learning and adaptive models are mentioned. They also check how the feeds on threat intelligence and the behavioral analytics are integrated into the SIEM systems to prevent risks. The evaluation wraps up with the future research directions, which are scalable, explainable and resilient prediction mechanisms needed to protect banking and FinTech ecosystems.**

Keywords—Forecasting Cyber Attacks, Banking Security, FinTech Platforms, Data-Driven Approaches, Machine Learning, Anomaly Detection, SIEM.

I. Introduction

The rapid growth of digital financial services, risks related to cybersecurity threats, and information privacy issues have grown. The increasing use of digital transactions, mobile banking, and cloud-based financial solutions has left FinTech companies vulnerable to cyberattacks, fraud, and regulatory issues [1]. The conventional risk management practices are ineffective at dealing with these advanced threats, so organizations have to incorporate the newest technologies, such as Artificial Intelligence (AI), to reinforce the security systems.

As cyber-attackers choose the easiest path with which to gain access to several sensitive areas and in filtrate the networks of an organization, financial institutions are becoming the primary target [2][3]. Cybercrime reports indicate that financial institutions are 300 times more likely to be the target of cyber-attacks than businesses in any other industry [4]. Therefore, cyber-attack prediction and forecasting are essential to prevent financial losses or reputational damage. A report prepared by the Online Trust Alliance on cyber-attack trends reported that the financial impact of such attacks in 2018 amounted to at least to $45 billion globally.

Through the use of machine learning algorithms and predictive analytics, AI can provide more fraud detection capabilities, track the trends of transactions, and detect possible vulnerabilities before exploitation [5][6]. AI is important in maintaining data privacy through automated compliance inspections, encryption of sensitive data, and the reduction of human error in security measures. The combination of AI and other technological innovations, including blockchain and biometric authentication, ensures an extra layer of protection against cybercrimes by enhancing FinTech security models.

Some of the other issues that have been brought about by this digital transformation are issues about cybersecurity, regulatory compliance, and risk management, among others [7][8]. The necessity to have strong, AI-optimized risk management systems has never been more urgent since financial services are becoming all-digital.

Machine learning and other Artificial Intelligence (AI) methods have since transformed the credit risk modeling [9]. Gradient boosting, neural networks, and ensemble algorithms have been shown to handle nonlinear patterns, adapt dynamically to changing data, and combine structured and unstructured information.

A. Structure of the Paper

The following is the structure of this review article. Section II discusses financial and FinTech threats in the cyber-world. Section III reviews data-driven methods for cyber-attack forecasting. The IV section deals with use in banking and FinTech security operations. Section V will summarize the collected literature, whereas Section VI will provide recommendations and future research directions.

II. Cyber Threat Landscape in Banking and FinTech Platforms

The threat of cyberattacks in the banking and FinTech domains is becoming more complex due to data breaches, phishing, ransomware, DDoS, supply-chain, and insider threats, which result from larger digital threat surfaces and interconnected ecosystems. These attacks are carried out by a wide range of entities, such as cybercriminals, nation-state-operated groups, hacktivists, and insiders, and therefore, proactive and data-driven prediction and protection systems are needed to protect financial systems.

- **Data Breaches and Unauthorized Access:** Within the vaults of finance platforms lie troves of sensitive client data, an enticing feast for cyber marauders. The Identity Theft Resource Center's sad count for 2021 - over 1,000 documented breaches serves as a monument to the persistent pursuit of unauthorized access, casting shadows over millions of records.

- **Phishing Attacks and Social Engineering:** The art of phishing orchestrates a misleading ballet, as cyber illusionists deploy emails, chats, and websites to mesmerize victims into inadvertently giving their secrets [10]. The Anti-Phishing Working Group's report paints a picture of dishonesty, demonstrating a 47% spike in these cyber masquerades in 2021, a striking dance of deception compared to the previous year.
- **Malware and Ransomware Threats:** The stage of financial operations witnesses a disruptive crescendo of malware and ransomware, a wicked symphony that exposes user data. As shown in Table I. The Cybersecurity and Infrastructure Security Agency's notes resonate with the crescendo of ransomware attacks targeting financial institutions, hitting both old banks and young fintech startups.

TABLE I. FREQUENCY AND FINANCIAL IMPACT OF VARIOUS CYBER THREATS OVER THE LAST FIVE YEARS

Year	Type of Cyber Threat	Number of Incidents	Financial Impact (in millions USD)
2020	Data Breaches	800	12.5
2020	Phishing Attacks	1200	8.2
2020	Ransomware Incidents	400	15.7
2019	Data Breaches	600	9.8
2019	Phishing Attacks	1,000	6.5
2019	Ransomware Incidents	300	11.2
2018	Data Breaches	500	7.3
2018	Phishing Attacks	800	5.1
2018	Ransomware Incidents	250	9.6

A. *Attack Surfaces in Digital Banking and FinTech Architectures*

In the fintech sector, cybersecurity strategies and solutions are essential as businesses battle more complex cyberthreats and work to preserve the security and confidence of their financial services [11]. Because fintech companies manage so much sensitive financial data, such as payment details, transaction history, and personal information, they have become easy targets for thieves (see Figure 1). Fintech organizations are using a range of proactive cybersecurity procedures and solutions to successfully reduce these threats.

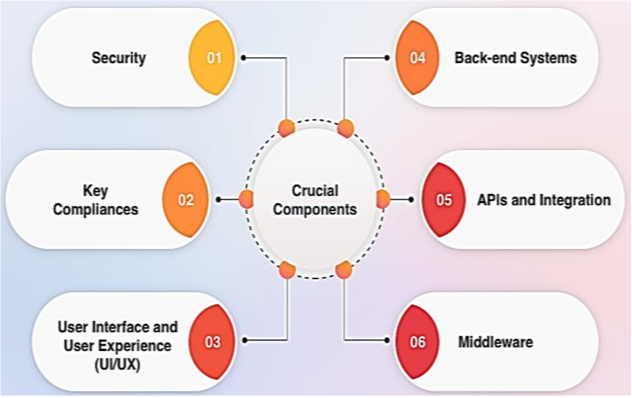

Fig. 1. Crucial components of Digital Banking architecture

1) *Advanced Security Protocols and Technologies*

Fintech companies are investing in the current security technology and procedures to make their defenses stronger. In addition to basic password methods, multi-factor authentication (MFA) is also widely employed to increase the level of access control. Although the logins might be stolen, MFA reduces the risk of unauthorized access by asking to provide additional verification criteria, such as biometrics or one-time passwords. Encryption is mandatory in the fintech systems to ensure data integrity as well as confidentiality during transit, and the rest [12]. Powerful encryption methods reduce the impact of data breaches, as it is impossible for unauthorized users to read personal information.

2) *Employee Training and Awareness*

Recognizing that human factors are a critical cybersecurity concern, fintech companies focus on comprehensive employee training and awareness initiatives. Employees are regularly trained on best cybersecurity practices, with particular emphasis on data security and potential threats such as phishing attacks. Employee knowledge is continually tested to ensure they are aware of recent cybersecurity threats and can effectively counter them. Fintech can empower employees to contribute towards maintaining the security of data and reducing potential risks by fostering a security culture.

3) *Data Protection Policies and Procedures*

In order to safeguard personal financial data in the fintech environment, the application of complex data protection regulations and processes is inevitable. Fintech can effectively mitigate risks and eliminate threats through continuous system surveillance, which enables early detection of anomalous behavior or potential security breaches [13]. Customer data is collected, stored, and shared under strict data management rules, reducing the possibility of illegal access or data leaks. Fintech organizations demonstrate their commitment to consumer trust by upholding regulatory compliance standards and upholding strict data security safeguards that secure customers' personal and financial information.

4) *Cloud Security Measures*

The growing use of cloud computing by finance for scalability and operational efficiency has made cloud environment security a top priority. Maintaining data integrity and security requires choosing trustworthy and secure cloud service providers. Fintech companies apply strong access controls, encryption techniques, and data segregation tactics inside cloud infrastructures to tailor cloud solutions to meet particular security requirements. Organizations may limit the inherent risks associated with cloud adoption and maintain the robustness of their financial services against possible cyber-attacks by implementing strict cloud security measures.

5) *API Security*

The integration and interoperability of fintech platforms greatly depend on Application Programming Interfaces (APIs). APIs need to be protected against potential vulnerabilities in order to secure sensitive data and maintain operations. To prevent the misuse of APIs and to reduce the severity of the impact of Distributed Denial of Service (DDoS) attacks, fintech companies apply techniques such as resource restrictions and rate limiting. API security is improved by putting strong authentication procedures and API gateways in place, which guarantee that only authorized parties may safely access and deal with sensitive financial data.

B. *Taxonomy of Cyber Attacks in Financial Systems*

Cyber threats targeting the banking and financial sectors have increased sharply since 2015, mainly due to the very fast and wide adoption of digital technology, the universal use of application programming interface (API) connectivity, and the ever-increasing rivalry between nations [14]. Moreover, it was pointed out that the financial sector experienced, between 2022 and 2023, a staggering 154% increase in major incidents like distributed denial of service (DDoS) attacks, which, thus, overtook the gaming industry as the most targeted sector; this is a clear indication that banks, insurers, and payment service providers are now at the center of the global cyber war.

The entire situation is compounded by these threats acting in unison to bring about a risk scenario that is very difficult to manage: ransomware, for instance, takes direct payments as a ransom, phishing prepares the ground for intruders by isolating them, DDoS attacks bring about a loss of confidence and cripple the establishment of the service, supply chain errors make the organization vulnerable, internal employee misconduct breeds distrust amongst the staff, and nation-state actors bring in their own strategic complexity.

The types of cybersecurity threats are:

1) Ransomware and Multi-Layer Extortion

Ransomware, however, still holds the title of the most financially damaging threat. Notorious ransomware gangs have established Ransomware as a Service (RaaS) platforms that allow non-expert but resourceful associates to launch and manage their campaigns for a fraction of the profits. Besides the siege in different ways, new gangs nowadays, for example, Co-Extortion, would not only encrypt and steal but also threaten the whole entire chain, thereby ensuring the victims would pay to avoid facing huge fines or suffering the loss of reputation [15]. It is reported that the amount received by LockBit through Bitcoin since the year 2022 is more than $200 million USD even after going through several arrests and raids.

2) Phishing, Social Engineering & Brand Impersonation

Credential-harvesting and malware-laden lures remain the dominant entry vectors because finance staff sit behind rich troves of customer data and payment rails. Attackers increasingly impersonate trusted brands such as DocuSign or SWIFT transfer notices; 68 per cent of counterfeit domains targeting finance are pure phishing sites [16]. The growth of adversaries-in-the-middle kits and AI-generated “deep-phish” Content lowers the barrier further, allowing criminals to sidestep MFA and initiate high-value wire fraud.

3) DDoS and Hacktivist Swarms

Layer 3/4 and application-layer DDoS attacks have resurged as a form of geopolitical “cyber-protest.” Financial services now absorb roughly one-third of all global DDoS traffic. Botnets driven by malware such as Mirai variants can marshal tens of millions of hijacked IoT devices.

4) Supply-Chain and Third-Party Platform Breaches

The 2023–24 MOVE it file-transfer compromise exposed a systemic blind spot: software used by thousands of firms worldwide can become a single point of failure [17]. Cl0p exploited a SQL-injection flaw, stealing data from more than 2,700 organizations, including global banks, credit unions, and payment processors, and exposing over 90 million personal records. A second wave in mid-2024 highlighted how sluggish patch uptake leaves loopholes open for encore attacks. Such incidents underscore how interconnected vendor ecosystems magnify risk far beyond any one institution’s perimeter.

C. Threat Actors and Attack Motivations

A threat actor is any person or group that intentionally targets digital environments, networks, or infrastructure through malicious activities to achieve specific objectives. This means they deliberately attack your systems, not always simply to cause random harm [18][19]. Many pursue specific objectives such as stealing data, disrupting operations, gaining financial benefits, conducting espionage, or accomplishing other strategic goals.

Types of threat Actors

1) Nation-state actors

Nation-state actors are government-sponsored groups that conduct cyber operations to advance their country's interests. These highly skilled adversaries have substantial resources, advanced tools, and often operate with legal protection from their sponsoring governments.

These actors typically focus on long-term intelligence gathering rather than quick financial gains. They might maintain access to your systems for months or years without being detected.

Key characteristics:

- **Extended presence:** They stay hidden in your systems for months or years to gather intelligence
- **Custom tools:** They often use bespoke malware and may leverage zero-day exploits, but also blend living-off-the-land techniques and commodity tools when it serves their goals.
- **Strategic targets:** They focus on critical infrastructure, government agencies, and organizations with valuable secrets.

2) Cybercriminals

Cybercriminals are financially motivated threat actors who range from individual operators to large crime organizations. Their primary goal is to make money from their attacks through various schemes.

The rise of ransomware-as-a-service has made it easier for less technical criminals to launch sophisticated attacks. They can now rent tools and infrastructure from other criminals, lowering the barrier to entry.

Common money-making tactics:

- **Ransomware attacks:** Encrypting your data and demanding payment for decryption keys, often combined with double extortion (threatening to leak stolen data) or triple extortion (targeting customers, partners, or other stakeholders)
- **Data theft:** Stealing sensitive information to sell on underground markets
- **Crypto jacking:** Using your computing resources to mine cryptocurrency without permission

3) Hacktivists

Hacktivists use cyberattacks to promote political or social causes. They want to raise awareness, embarrass targets, or disrupt the operations of organizations they oppose.

Unlike financially motivated actors, hacktivists care more about spreading their message than making money. Their attacks often happen during political events, social movements, or public controversies.

Typical activities:

- **Website defacement:** Replacing legitimate website content with political messages

- **Data leaks:** Exposing sensitive information can damage a target's reputation
- **DDoS attacks:** Overwhelming servers with traffic to disrupt services

4) *Insider threats*

Insider threats come from people with legitimate access to your systems who misuse their privileges. These threats are especially hard to detect because they operate within normal access patterns and bypass traditional security defenses.

Categories of insider threats:

- **Malicious insiders:** Current or former employees who intentionally steal data or sabotage systems.
- **Negligent insiders:** Employees who accidentally create security risks through careless actions.
- **Compromised insiders:** Legitimate accounts taken over by external threat actors.

III. Data-Driven Approaches for Cyber-Attack Forecasting

Cyber-attacks are sophisticated, and this model aims to help predict cyber-attack events. The proactive approaches will help security teams and senior managers implement approaches that protect their network systems [20]. It leveraged a publicly available dataset that contains multiple attack labels collected from a realistic and secure network.

- **Data Preparation:** The dataset that was utilized was generated from a realistic network and is called CSE-CIC-IDS2018. As seen in Figure 2, the stages of dataset preparation and experimentation include dataset preparation and feature selection, classification, time series forecasting, and performance evaluation.

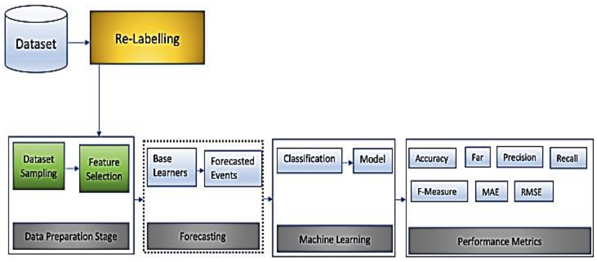

Fig. 2. Forecasting Stages

- **Attack Classification:** Supervised learning to classify and categorize the observations. The attack classification was performed after the forecasting was completed. It applied popular classification algorithms such as Bayes Net, Naive Bayes, k-NN, Support Vector Machine (SVM) and random forest.

A. *Machine Learning–Based Forecasting Models*

Machine Learning algorithms are mainly divided into four categories: Supervised learning, Unsupervised learning, Semi-supervised learning, and Reinforcement learning.

1) *Supervised*

Supervised learning is typically the task of machine learning to learn a function that maps an input to an output based on sample input-output pairs. It uses labelled training data and a collection of training examples to infer a function. Supervised learning is carried out when certain goals are identified to be accomplished from a certain set of inputs, i.e., a task-driven approach [21]. The most common supervised tasks are classification, which separates the data, and regression, which fits the data. For instance, predicting the class label or sentiment of a piece of text, like a tweet or a product review, i.e., text classification, is an example of supervised learning.

2) *Unsupervised*

Unsupervised learning analyzes unlabeled datasets without the need for human interference, i.e., a data-driven process. This is widely used for extracting generative features, identifying meaningful trends and structures, groupings in results, and exploratory purposes. The most common unsupervised learning tasks are clustering, density estimation, feature learning, dimensionality reduction, finding association rules, anomaly detection, etc.

B. *Hybrid and Ensemble Forecasting Methods*

A hybrid CNN-LSTM model is the last DL ensemble method. Very long input sequences can be handled as blocks or subsequences, as the hybrid model contains both CNN and LSTM models. In this case, the sequential data are divided into further subsequences for each sample to train the hybrid model [22]. A hybrid structure of CNN and LSTM models is represented in Figure 3. Primarily, the CNN model interprets each subsequence of sequential inputs. In this case, the CNN model is enveloped in Time Distributed wrapper layers of convolution, pooling, and flattening [23]. Hereafter, the results are assembled by the LSTM layer before making a test prediction. The parameters of the hybrid model are adjusted in the same way as those of stand-alone CNN and LSTM models.

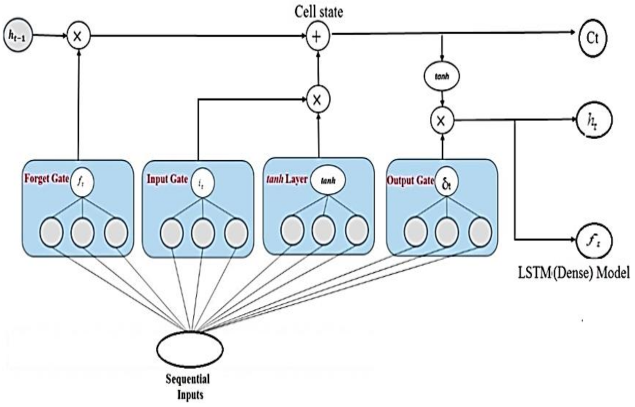

Fig. 3. Hybrid CNN-LSTM model

Gradient Boosting is an ML model for regression and classification problems that produces a prediction model as an ensemble of weak learners, typically decision trees. It builds the model stage-wise, as other boosting models do, and it generalizes them by allowing optimization of an arbitrary differentiable loss function.

The idea behind the GBR approach is that boosting can be interpreted as an optimization algorithm with respect to a suitable cost function. The algorithm optimizes a cost function over the function space by iteratively selecting a function (weak hypothesis) that moves in the negative gradient direction. This functional gradient view of boosting has led to the development of boosting algorithms in machine learning and statistics beyond regression and classification.

The Automatic Relevance Determination (ARD) model, also known as Sparse Bayesian Learning or Relevance Vector Machine, is a type of Bayesian linear regression [24]. It imposes a prior distribution on the weights, leading to automatic sparsity and relevance determination of features.

Let us denote the design matrix (with n samples and m features) as $X \in \mathbb{R}^{n\times m}$and the corresponding target values as $y \in \mathbb{R}^{n}$. They also denote the weight vector as $w \in \mathbb{R}^{m}$. The linear model can be represented in an Equation. (1) as:

$$y = Xw + \epsilon \tag{1}$$

where $\epsilon$is the noise term, assumed to follow a Gaussian distribution with zero mean and variance σ^2 , i.e., $\epsilon \sim N(0, \sigma^2)$. In ARD, each weight w_i in w is assumed to follow a Gaussian distribution with zero mean and its own variance α_i^{-1}, defined in Equation. (2) as:

$$w_i \sim N(0, \alpha_i^{-1}) \tag{2}$$

The ARD model aims to find the Maximum a posteriori (MAP) estimates of the weights, w^*, and the hyperparameters $\alpha^*$and σ^{*2}, defined in Equation. (3):

$$w^*, \alpha^*, \sigma^{*2} = \arg\max_{w,\alpha,\sigma^2} p(w, \alpha, \sigma^2 | y) \tag{3}$$

This maximization problem can be solved iteratively using Expectation-Maximization or similar optimization algorithms. When α_i becomes very large, the corresponding weight, w_i , is pushed towards zero, leading to automatic sparsity.

IV. Applications in Banking and FinTech Security Operations

FinTech platforms are vulnerable to cybersecurity attacks, such as service interruption, data breaches, financial fraud, and new vectors of attacks, which prove to be of high operational, financial, and regulatory risks. FinTech faces various security threats as:

- **Cybersecurity threats:** These threats involve malicious activities that disrupt services or steal sensitive information from FinTech applications [25]. The consequences can include financial losses and punitive actions from government authorities.
- **Fraud:** Fraudulent activities in FinTech often involve unauthorized transactions, identity theft, and unauthorized access to accounts, leading to significant financial and reputational damage.
- **Emerging threats:** As technology evolves, new threats continuously emerge, requiring ongoing vigilance and adaptation by FinTech companies to safeguard their systems and users

A. Fraud Prevention and Risk Scoring

Fraud risk scoring is an analytical approach employed to assess the likelihood of a transaction or activity being fraudulent, based on a predefined set of criteria and data points. Each event or action can be assigned a risk score based on user behaviour, transaction history, and network connections. This risk score indicates the probability of the event or action being fraudulent [26]. These scores enable organisations to detect suspicious patterns, trace abnormalities, and take informed decisions on subsequent actions to either authorize or block a transaction.

This technique uses statistics, machine learning, and artificial intelligence to accurately assess and continuously update fraudsters' changing strategies [27]. In essence, Fraud Risk Scoring serves as an early warning system for businesses, enabling them to proactively identify and mitigate potential risks before they escalate into serious threats, saving both resources and reputational damages in the process.

Fraud risk scoring utilizes a combination of techniques to assess and predict the likelihood of fraudulent activities. Some of these techniques include:

- **User behaviour analysis:** Understanding user patterns allows businesses to detect unusual actions that may indicate potential fraud. This includes tracking login attempts, browsing behaviour, and purchase history to establish a comprehensive user profile.
- **Transaction history monitoring:** Examining past transactions can uncover discrepancies and help identify risky behaviour. Consistent order amounts, irregular locations, and repetitive purchase patterns are some of the red flags that can be detected through transaction history analysis.
- **IP address tracking:** Identifying and analyzing IP addresses associated with transactions can reveal patterns indicative of fraud attempts. Factors such as multiple transactions from a single IP address or geolocation inconsistencies can further raise suspicions.
- **Email address scrutiny:** Evaluating email addresses can help determine user legitimacy and expose suspicious activity. Unusual domain names, uncommon email patterns, or a high volume of recently created email accounts can be warning signs.

B. Intrusion Detection and Threat Anticipation

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them [28][29]. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process.

When adversaries attack a system, they typically do so in predictable stages:

The first stage of an attack is usually probing or examining a system or network to find an optimal point of entry. In systems without an IDS, the attacker can thoroughly examine the system with little risk of detection or retaliation. Given this unfettered access, a determined attacker will eventually find a vulnerability in such a network and exploit it to gain entry to various systems.

The same network with an IDS monitoring its operations presents a much more formidable challenge to that attacker. Although the attacker may probe the network for weaknesses, the IDS will observe the probes, identify them as suspicious, may actively block the attacker's access to the target system, and will alert security personnel who can then take appropriate actions to block subsequent access by the attacker. Even the presence of a reaction to the attacker's probing of the network will elevate the level of risk the attacker perceives, discouraging further attempts to target the network.

C. *Security Information and Event Management (SIEM) Integration*

Security Information and Event Management (SIEM) systems have been developed in response to help administrators to design security policies and manage events from different sources. Generally, a simple SIEM is composed of separate blocks (e.g., source device, log collection, parsing normalization, rule engine, log storage, event monitoring) that can work independently from each other, but without them all working together, the SIEM will not function properly. Figure 4 depicts the basic components of a regular SIEM solution.

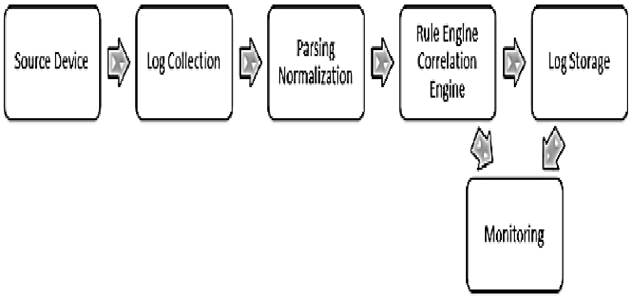

Fig. 4. SIEM basic components

SIEM platforms provide real-time analysis of security events generated by network devices and applications[30]. In addition, even though the new generation of SIEMs provides response abilities to automate the process of selecting and deploying countermeasures, current response systems select and deploy security measures without performing a comprehensive impact analysis of attacks and response scenarios. Besides these common features, current SIEMs present differences that classify them as leaders, challengers, niche players, or visionaries, according to Gartner's SIEM Magic Quadrant annual report.

V. Literature Review

The evaluated literature identifies the increasing cyber threats in fintech because of digitalization. Machine learning and AI, such as predictive models, deep learning, and others, improve the identification of threats, anomalies, and even prevent fraud. As shown in Table II. Cybersecurity proactive measures enhance real-time response, and future efforts should need adaptable, expanding, and unified response to future threats.

Busari et al. (2025) rapid digitization of financial services in the United States has significantly increased the volume and sensitivity of consumer data processed by fintech platforms. This evolution has simultaneously elevated the risk and sophistication of cyber threats targeting these systems. This explores the role of artificial intelligence (AI)-driven threat detection systems in enhancing real-time consumer data security within the US fintech sector. The study investigates the integration of machine learning algorithms, behavioral analytics, and anomaly detection in proactively identifying and neutralizing cyber threats. Through a comprehensive analysis of current AI-based security architectures and case studies from leading US fintech firms, the research highlights the strengths and limitations of existing approaches [31].

Kokogho et al. (2025), by leveraging these technologies, organizations can build proactive defenses, improve threat detection accuracy, and reduce response times to cyber incidents. Advanced analytics enable fintech companies to process large volumes of real-time data, identifying anomalies and potential vulnerabilities with unparalleled precision. Techniques such as predictive modeling and behavior analysis allow for the early detection of sophisticated threats, including phishing, ransomware, and advanced persistent attacks. Machine learning algorithms enhance these capabilities by continuously learning from evolving cyber threats, adapting to new attack vectors, and optimizing detection mechanisms. Incorporating machine learning into cybersecurity risk management frameworks also facilitates automated responses to identified threats [32].

Ramrakhyani and Shrivastava (2024) financial technology (fintech) sector has witnessed remarkable expansion in recent years, fundamentally reshaping the landscape of financial services delivery and consumption. This growth is driven by new technologies such as mobile banking, digital wallets, blockchain and artificial intelligence. The risk for fintech has increased. As pioneers in the use of technology to enhance financial transactions, Fintech has become an attractive target for cybercriminals looking to exploit weaknesses in digital infrastructure. The evolving nature and sophistication of cyber threats, including phishing attacks, ransomware, data breaches, and insider threats, pose significant risks to the integrity and security of financial data and assets [33].

Bilipelli et al. (2023) fast-paced digitalizing financial landscape, cyberattacks against FinTech platforms become more complex and pose an ever-increasing threat to their operations. To meet the necessities of a proper and timely threat prediction, the proposed study presents the Alert BERT, a transformer-based deep learning model specialized in predicting the evolution of cyber threats within FinTech. The model is trained using robust preprocessing with the help of the IEEE-CIS fraud dataset, in which data cleaning, normalization, categorical encoding, and SMOTE-based class balancing are performed. Alert BERT uses the contextual learning ability of BERT on the structured transaction data and is capable of capturing sequential patterns of cyber threats [34].

Qasaimeh et al. (2022), as the number of cyber-attacks on financial institutions has increased over the past few years, an advanced system that is capable of predicting the target of an attack is essential. Such a system needs to be integrated into the existing detection systems of financial institutions as it provides them with proactive controls with which to halt an attack by predicting patterns. Advanced prediction systems also enhance the software design and security testing of new advanced cybersecurity measures by providing new testing scenarios supported by attack forecasting [35].

Williams, Yussuf and Olukoya (2021) cyberattacks and fraudulent schemes have grown increasingly advanced, rendering traditional defense mechanisms insufficient. Machine learning (ML) has emerged as a groundbreaking solution, enabling organizations to conduct proactive risk assessments and prevent fraudulent activities. By harnessing sophisticated algorithms, ML facilitates the identification of threats, anomaly detection, and timely responses, ensuring the protection of digital financial infrastructures. Advanced cybersecurity risk evaluation utilizes ML techniques such as supervised learning for detecting predefined attack patterns, unsupervised learning for recognizing unusual behaviors, and reinforcement learning for refining countermeasure strategies [36].

TABLE II. COMPARATIVE ANALYSIS OF DIGITAL TWIN–BASED PREDICTIVE MAINTENANCE APPROACHES IN INDUSTRIAL SYSTEMS

Authors (Year)	Focus Area	Key Findings	Approaches	Objectives	Future Work
Busari et al. (2025)	AI-driven threat detection in US fintech	AI-based systems enhance real-time security, but have limitations; integration of ML and behavioral analytics improves threat detection	Machine learning algorithms, behavioral analytics, anomaly detection	Explore AI integration to proactively detect and neutralize cyber threats in fintech	Improve existing AI architectures; address limitations in scalability and adaptability
Kokogho et al. (2025)	Proactive cybersecurity in fintech	Advanced analytics and ML enable faster threat detection and automated responses; reduce downtime and financial loss	Predictive modeling, behavior analysis, ML-based automated response	Build proactive defenses and improve detection accuracy in fintech	Develop more adaptive models for evolving cyber threats
Ramrakhyani & Shrivastava (2024)	Cybersecurity strategies in fintech	Fintech growth increases cyber risk; threats include phishing, ransomware, data breaches, and insider threats	Literature review of cybersecurity measures	Provide a comprehensive review of cybersecurity strategies in fintech	Suggest the development of holistic and adaptive security frameworks for fintech
Bilipelli et al. (2023)	Predictive modeling for fintech cyber threats	Alert BERT model effectively predicts cyber threat evolution using contextual learning; captures sequential patterns in transaction data	Transformer-based deep learning (BERT), IEEE-CIS fraud dataset, data preprocessing, SMOTE class balancing	Develop a predictive model for timely threat detection in fintech	Extend the model to other fintech datasets and real-time deployment
Qasaimeh et al. (2022)	Forecasting network-based cyber-attacks	Deep neural network model forecasts attack targets, enhances proactive controls, and improves security testing	Deep neural networks, attack pattern forecasting	Predict future cyber-attacks on financial institutions to improve defenses	Integrate predictive models with live detection systems; enhance forecasting accuracy
Williams, Yussuf and Olukoya (2021)	ML for fraud detection & proactive cybersecurity	ML enables proactive risk assessment, anomaly detection, and fraud prevention; improves adaptation to evolving threats	Supervised, unsupervised, reinforcement learning for threat detection and countermeasures	Strengthen forecasting and prevention of cyber threats and fraud in financial systems	Refine ML models to handle complex, evolving cyber threats and large datasets

VI. CONCLUSION AND FUTURE WORK

The current dynamic of cyber threats within the banking and FinTech platforms highlighting the increasing significance of data-driven predictive models of proactive security management. Through a methodological review of the available literature, the research has highlighted the use of machine learning, deep learning, and statistical modeling techniques to detect and predict cyberattacks at an early stage using behavioral analysis, anomaly detection, and threat intelligence fusions. The results show that data-driven techniques greatly improve situational awareness, response time and resilience of financial systems to more advanced and dynamic attack vectors. Nevertheless, issues with the quality of data and the understandability of models, scalability, and compliance with regulations are all serious barriers to practical implementation. On the whole, the review highlights that predicting cyber-attacks is an essential aspect of the current banking and FinTech security practice, between the mechanisms of response to security threats and the forecast of the risk of these threats. Such methods should be reinforced to guarantee safe, reliable and stable digital financial ecosystems.

The research of the future needs to be aimed at the creation of explainable and privacy-preserving forecasting systems, the incorporation of real-time threat detection, and the application of federated and hybrid learning capabilities. Also, the extensive validation of it with real-world financial data and compliance with regulatory frameworks will be an essential step towards practical implementation.

REFERENCES

[1] F. Akram and M. Sameer, "AI-Driven Risk Assessment in FinTech: Strengthening Cybersecurity and Data Privacy," 2025. doi: 10.13140/RG.2.2.28036.85121.

[2] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 3, p. 12, Jan. 2024, doi: 10.52866/ijcsm.2024.05.03.004.

[3] H. P. C. Kapadia, "Role-Based Access Control (RBAC) for Banking Web Platforms: Compliance Implications," *Int. J. Nov. Trends Innov.*, vol. 1, no. 3, pp. 11–15, 2023.

[4] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[5] C. Hall and J. Cole, "Data-Driven Approaches for Fraud Prevention in Online Banking," 2024.

[6] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[7] C. I. Samson-Onuorah, "AI-driven Credit Risk Modeling: Leveraging Big Data Analytics to Improve Financial Stability and Lending Efficiency in Banks," *Int. J. Sci. Eng. Appl.*, vol. 14, no. 10, pp. 57–70, Sep. 2025, doi: 10.7753/IJSEA1410.1009.

[8] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[9] F. Akram and N. Rahman, "The Future of Digital Finance: AI in Banking, Fintech Innovation, and Data Security for Financial Inclusion and Regulatory Compliance," 2025. doi: 10.13140/RG.2.2.35984.93447.

[10] P. Kamuangu, "A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends," *J. Econ. Financ. Account. Stud.*, vol. 6, no. 1, pp. 47–53, Feb. 2024, doi: 10.32996/jefas.2024.6.1.5.

[11] T. Kamlakshya, "Enhancing cybersecurity in digital banking transformation: A framework for secure payment ecosystems," *World J. Adv. Eng. Technol. Sci.*, vol. 10, no. 2, pp. 441–448, Dec. 2023, doi: 10.30574/wjaets.2023.10.2.0309.

[12] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo, "Cybersecurity strategies in fintech: safeguarding financial data and assets," *GSC Adv. Res. Rev.*, vol. 20, no. 1, pp. 050–056, Jul. 2024, doi: 10.30574/gscarr.2024.20.1.0241.

[13] S. B. Shah, "Evaluating the Effectiveness of Machine Learning in Forecasting Financial Market Trends: A Fintech Perspective," in *2025 3rd International Conference on Integrated Circuits and*

Communication Systems (ICICACS), IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/ICICACS65178.2025.10968297.

[14] A. Bello, I. Wonuola, A. Izundu, and J. Izundu, "Cybersecurity threats in the financial sector: Analyzing attack types, Vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024)," *Int. J. Sci. Res. Arch.*, vol. 16, no. 1, pp. 134–150, Jul. 2025, doi: 10.30574/ijsra.2025.16.1.2007.

[15] T. Shah, "The Role of Customer Data Platforms (CDPs) in Driving Hyper-Personalization in FinTech," *Int. Res. J. Eng. Technol.*, vol. 12, no. 04, p. 10, 2025.

[16] T. Pseftelis and G. Chondrokoukis, "Cyber Attack Motivations: Connecting Actors with Event Types," May 13, 2025. doi: 10.20944/preprints202505.1003.v1.

[17] G. Rabitti, A. Khorrami Chokami, P. Coyle, and R. D. Cohen, "A taxonomy of cyber risk taxonomies," *Risk Anal.*, vol. 45, no. 2, pp. 376–386, Feb. 2025, doi: 10.1111/risa.16629.

[18] Z. A. El Houda, "Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape," in *Cyber Security for Next-Generation Computing Technologies*, CRC Press, 2024, pp. 84–101.

[19] S. B. Karri, S. Gawali, S. Rayankula, and P. Vankadara, "AI Chatbots in Banking: Transforming Customer Service and Operational Efficiency," in *Advancements in Smart Innovations, Intelligent Systems, and Technologies*, 2025. doi: 10.3233/FAIA251498.

[20] Y. Ahmed, M. A. Azad, and T. Asyhari, "Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features," *Information*, vol. 15, no. 1, Jan. 2024, doi: 10.3390/info15010036.

[21] R. Pugliese, S. Regondi, and R. Marini, "Machine learning-based approach: global trends, research directions, and regulatory standpoints," *Data Sci. Manag.*, vol. 4, pp. 19–29, Dec. 2021, doi: 10.1016/j.dsm.2021.12.002.

[22] P. P. Phyo and Y.-C. Byun, "Hybrid Ensemble Deep Learning-Based Approach for Time Series Energy Prediction," *Symmetry (Basel)*, vol. 13, no. 10, Oct. 2021, doi: 10.3390/sym13101942.

[23] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis: A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[24] H. Wu and D. Levinson, "The ensemble approach to forecasting: A review and synthesis," *Transp. Res. Part C Emerg. Technol.*, vol. 132, Nov. 2021, doi: 10.1016/j.trc.2021.103357.

[25] S. E. V. S. Pillai and W.-C. Hu, "Security and Privacy Challenges and Opportunities in FinTech," in *2024 Cyber Awareness and Research Symposium (CARS)*, IEEE, Oct. 2024, pp. 1–6. doi: 10.1109/CARS61786.2024.10778753.

[26] S. Metha, "AI-Driven Fraud Detection: A Risk Scoring Model for Enhanced Security in Banking," *J. Eng. Res. Reports*, vol. 27, no. 3, pp. 23–34, Feb. 2025, doi: 10.9734/jerr/2025/v27i31415.

[27] V. Shewale, "The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 15, pp. 11–20, Apr. 2025, doi: 10.37745/ejcsit.2013/vol13n151120.

[28] A. Londhe, S. Gawathe, P. Pandey, G. Date, and S. Meshram, "Intrusion Detection System," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 31–35, Apr. 2024, doi: 10.48175/IJARSCT-17606.

[29] A. Parupalli, "Business Intelligence in ERP: ML-Based Comparative Study for Financial Forecasting," *ESP Int. J. Adv. Comput. Technol.*, vol. 2, no. 4, pp. 17–26, 2024, doi: 10.56472/25839217/IJCEET-V2I4P103.

[30] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144759.

[31] M. Busari, "AI-Driven Threat Detection Systems in US Fintech: Enhancing Real-Time Consumer Data Security," 2025.

[32] E. Kokogho, R. Okon, B. M. Omowole, C. P.-M. Ewim, and O. C. Onwuzulike, "Enhancing cybersecurity risk management in fintech through advanced analytics and machine learning," *Gulf J. Adv. Bus. Res.*, vol. 3, no. 2, pp. 1–30, 2025.

[33] A. Ramrakhyani and N. K. Shrivastava, "Artificial Intelligence: Revolutionizing the Future of Fintech," *Commer. Res. Rev.*, vol. 1, no. 2, pp. 10–22, 2024.

[34] A. R. Bilipelli, "Forecasting the Evolution of Cyber Attacks in FinTech Using Transformer-Based Time Series Models," *Int. J. Res. Anal. Rev.*, vol. 10, no. 3, pp. 383–389, 2023.

[35] 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," *J. Softw. Evol. Process*, vol. 34, no. 11, Nov. 2022, doi: 10.1002/smr.2489.

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