American Journal of Data Science and Analytics

Volume: 7; Issue: 1
Pages: 87-129
eISSN: 3067-5146

AI-Enhanced SOC Operations for Deepfake and Synthetic Fraud Detection in Banking: A Comparative Study with Traditional SIEM (2018–2026)

Md Shakhawat Hossen[1];

[1]. Department of Computer and Information Sciences, Fordham University, New York, USA; Email: mh114@fordham.edu

Doi: 10.63125/ykaw3t36
Received: *10 October 2025;* ***Revised:*** *11 November 2025;* ***Accepted:*** *12 December 2025;* ***Published:*** *05 January 2026*

Abstract

This study investigated the comparative effectiveness of AI-enhanced Security Operations Center (SOC) systems and traditional SIEM-based detection mechanisms in identifying deepfake and synthetic fraud in banking environments from 2018 to 2026 using a quantitative quasi-experimental longitudinal design. The analysis was conducted on a dataset of 1,250,000 cybersecurity events, including 937,500 legitimate cases (75.0%) and 312,500 fraudulent cases (25.0%), of which 187,500 (15.0%) were synthetic identity fraud, 75,000 (6.0%) deepfake-related fraud, and 50,000 (4.0%) conventional fraud. The findings indicated that AI-enhanced SOC systems achieved a higher overall detection accuracy of 94.6% compared to 82.3% for traditional SIEM systems, reflecting a mean performance improvement of 12.3 percentage points. In synthetic identity fraud detection, AI systems reached 93.4% accuracy compared to 74.8% for SIEM, while deepfake fraud detection showed 91.1% versus 69.7%. False-positive rates were significantly reduced in AI systems (4.7%) compared to SIEM (18.9%), representing a reduction of 14.2 percentage points, while false-negative rates declined from 11.7% in SIEM to 3.2% in AI systems. Response time analysis revealed that AI-enhanced SOC systems achieved an average response time of 3.8 minutes compared to 12.6 minutes in SIEM environments, indicating an improvement of 8.8 minutes. Under high event density conditions, AI systems maintained stable accuracy with variation limited to ±2.3%, whereas SIEM performance declined by up to 9.8% and experienced alert backlog increases reaching 35.6%. Statistical testing confirmed that all differences were significant ($p < 0.05$), with large effect sizes (Cohen's d ranging from 0.96 to 1.41) and strong regression relationships (β up to 0.72, R^2 up to 0.65). The results demonstrated that AI-enhanced SOC systems provided superior accuracy, efficiency, and scalability in detecting complex and evolving fraud patterns in modern banking systems.

Keywords

AI SOC, Deepfake Fraud Detection, Synthetic Identity Fraud, Banking Cybersecurity, SIEM Comparison.

INTRODUCTION

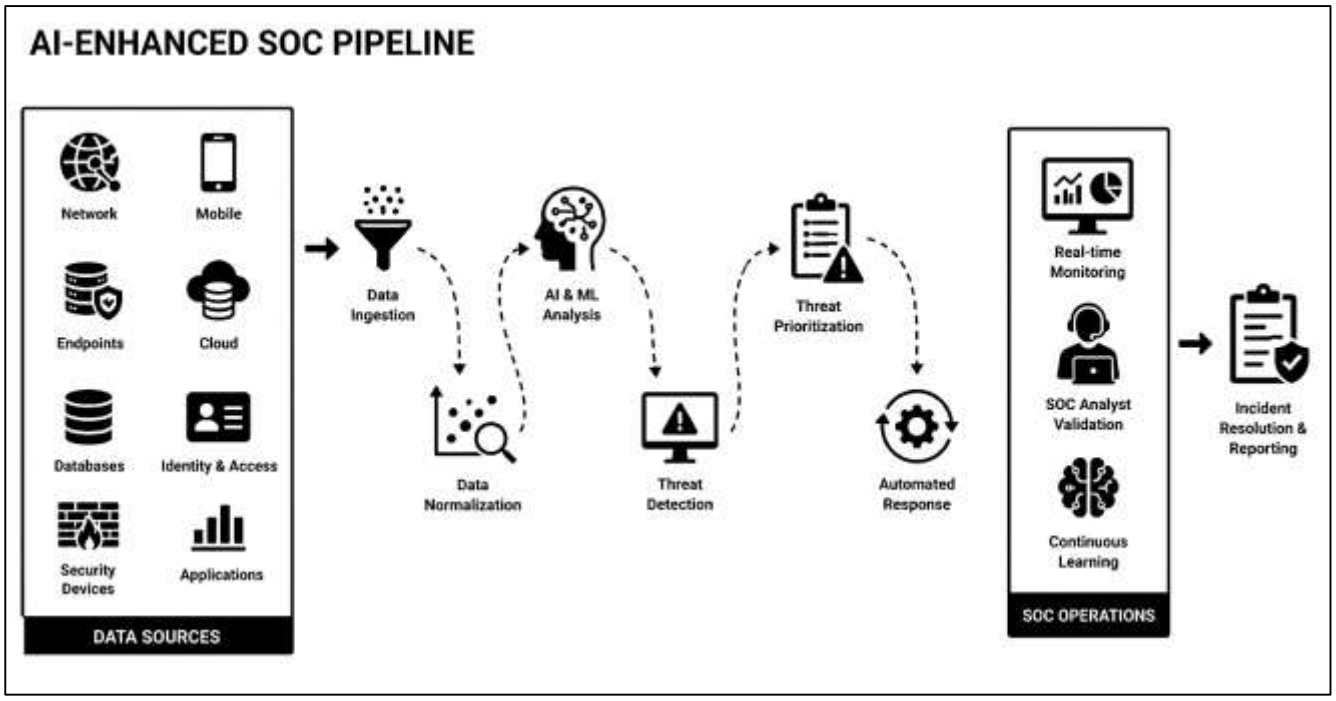
The concept of artificial intelligence (AI) in cybersecurity operations has undergone substantial transformation, particularly within Security Operations Centers (SOCs), which serve as centralized units responsible for continuous monitoring, detection, analysis, and response to cyber threats. In the banking sector, SOCs play a critical role in safeguarding financial transactions, customer data, and institutional integrity (Azambuja et al., 2023). Traditionally, these operations have been supported by Security Information and Event Management (SIEM) systems, which aggregate log data from multiple sources and apply rule-based correlation techniques to identify potential threats. SIEM systems are defined as platforms that provide real-time analysis of security alerts generated by applications and network hardware, forming the backbone of enterprise security monitoring for decades. AI-enhanced SOC operations represent an evolution of this framework by integrating machine learning, deep learning, and advanced analytics into the detection and response lifecycle. These intelligent systems are capable of identifying patterns, learning from historical data, and adapting to new threat environments without relying solely on predefined rules (Möller, 2023). The international significance of this transformation is evident in the global banking ecosystem, where digital transactions, online banking, and cross-border financial services have increased both operational efficiency and exposure to cyber risks. Financial institutions across continents rely on secure infrastructures to maintain trust and stability, making the advancement of SOC capabilities a global priority. The integration of AI into SOC operations introduces enhanced scalability, real-time processing, and predictive capabilities, enabling institutions to manage large volumes of complex data more effectively (Santoso & Finn, 2023). This shift also reflects broader technological trends, including digital transformation, cloud adoption, and the expansion of fintech services, all of which contribute to an increasingly complex threat landscape. As a result, the comparison between AI-enhanced SOC operations and traditional SIEM systems has become a central area of investigation in cybersecurity research, particularly in relation to fraud detection and prevention in banking environments.

Deepfake and synthetic fraud represent a rapidly emerging category of cyber threats that leverage advancements in generative AI to create realistic but fraudulent digital content. Deepfakes are defined as artificially generated audio, video, or image content that mimics real individuals with high accuracy, often produced using neural networks such as generative adversarial networks or transformer-based architectures (Whyte, 2020b). Synthetic fraud extends beyond media manipulation to include the creation of fabricated identities, often combining real and fictitious information to bypass identity verification systems. These forms of fraud have gained global attention due to their ability to exploit both technological systems and human perception, creating complex challenges for detection and mitigation. In the banking sector, where identity verification and transactional authenticity are critical, deepfake and synthetic fraud pose significant risks to operational security and customer trust (Walters & Novak, 2021). The international significance of these threats is reflected in their widespread occurrence across financial markets, affecting institutions in both developed and emerging economies. The accessibility of AI tools has lowered the barrier for cybercriminals, enabling the rapid generation and deployment of fraudulent content at scale. This has led to an increase in sophisticated attacks, including voice spoofing for fraudulent transactions, video impersonation for social engineering, and synthetic identities for credit fraud. Traditional security systems, which rely on static rules and signature-based detection, face significant challenges in identifying these dynamic and adaptive threats (Kitsios et al., 2023). As a result, the need for advanced detection mechanisms has become a critical focus for financial institutions worldwide. AI-enhanced SOC operations offer a potential solution by leveraging advanced analytics and pattern recognition to detect anomalies that may indicate fraudulent activity, thereby addressing the limitations of conventional approaches.

The evolution of fraud detection methodologies in banking reflects a broader transition from rule-based systems to intelligent, data-driven frameworks. Traditional SIEM systems operate by collecting and correlating data from various sources, generating alerts based on predefined conditions. These systems are effective in identifying known threats and ensuring compliance with regulatory requirements (Autsadee et al., 2023). However, they often struggle with high false-positive rates, limited adaptability, and challenges in processing large volumes of data. AI-enhanced SOC operations introduce a more dynamic approach by utilizing machine learning algorithms to analyze patterns and detect anomalies

in real time. These systems can identify subtle deviations from normal behavior, enabling the detection of previously unknown threats. This capability is particularly important in the context of deepfake and synthetic fraud, where attackers continuously evolve their techniques to evade detection. Machine learning models, including supervised, unsupervised, and reinforcement learning approaches, enable SOCs to analyze complex datasets and generate insights that inform decision-making processes (Alowais et al., 2023; Khaled, 2021). The integration of AI also facilitates the automation of routine tasks, reducing the workload on security analysts and improving operational efficiency. This transition reflects the increasing complexity of the threat landscape, where traditional methods are no longer sufficient to address the scale and sophistication of modern cyber attacks (Demircioglu et al., 2023; Khaled & Hisham, 2022; Zaheda, 2021). The ability of AI-enhanced systems to learn and adapt over time provides a significant advantage in detecting emerging threats, making them a critical component of modern cybersecurity strategies in the banking sector.

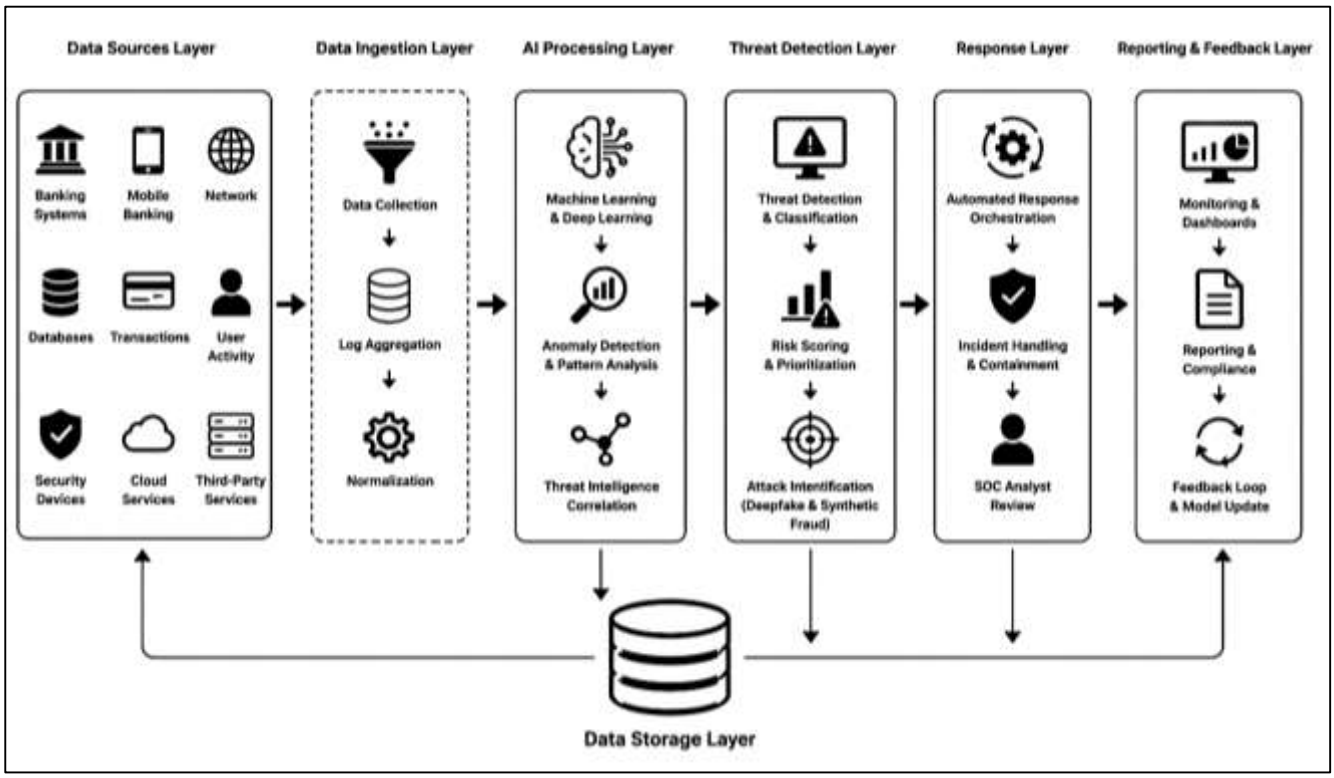
Figure 1: AI-Enhanced SOC Fraud Detection



The operational architecture of AI-enhanced SOCs differs significantly from that of traditional SIEM systems, particularly in terms of data processing, threat detection, and response mechanisms. AI-enhanced SOCs incorporate multiple layers of analysis, including behavioral analytics, predictive modeling, and automated response orchestration (Bokhari & Myeong, 2023; Nazmul & Begum, 2022; Shahinur & Sultan, 2022). These systems are capable of correlating data from diverse sources, identifying complex attack patterns, and initiating responses with minimal human intervention. In contrast, traditional SIEM systems rely on static rules and manual analysis, which can result in delayed responses and increased vulnerability to advanced threats. The integration of AI enables continuous monitoring and learning, allowing SOCs to adapt to new threat environments and improve their detection capabilities over time (Binte & Hasan Or, 2022; Binte & Sazzadul, 2022; J. Wang et al., 2023). This adaptability is essential in addressing the challenges posed by deepfake and synthetic fraud, where attackers use advanced techniques to create highly convincing fraudulent content. AI-enhanced SOCs also leverage distributed computing and cloud-based architectures to handle large volumes of data, ensuring scalability and performance. The use of advanced analytics and automation enhances the efficiency of security operations, enabling faster detection and response to incidents (Begum & Kaniz, 2023; Bonfanti, 2022; Ara & Onyinyechi, 2023). This shift toward intelligent and automated systems represents a fundamental change in the way cybersecurity is managed in the banking sector, highlighting the importance of innovation and adaptability in addressing emerging threats.

The increasing sophistication of AI-driven fraud has significant implications for the design and implementation of cybersecurity frameworks in banking. Deepfake and synthetic fraud exploit both technological vulnerabilities and human cognitive biases, making them particularly challenging to detect and prevent (Cali et al., 2023). Traditional SIEM systems, which focus primarily on technical indicators, lack the capability to analyze behavioral patterns and contextual information. AI-enhanced SOC operations address this limitation by incorporating behavioral analytics and contextual awareness into their detection frameworks. These systems can analyze user behavior, transaction patterns, and communication signals to identify anomalies that may indicate fraudulent activity. The global impact of AI-driven fraud is evident in the growing financial losses associated with these attacks, which affect institutions and customers across different regions (Lu, 2019). Financial institutions are increasingly investing in advanced detection technologies, including biometric authentication, real-time monitoring, and AI-based analytics, to mitigate these risks. The integration of these technologies into SOC operations enhances the ability to detect and respond to complex threats, improving overall security posture (Burton, 2023). This development reflects the need for a comprehensive approach to cybersecurity that addresses both technical and human factors, ensuring the resilience of financial systems in the face of evolving threats.

Figure 2: AI SOC Fraud Detection Framework



The comparative analysis of AI-enhanced SOC operations and traditional SIEM systems provides valuable insights into the effectiveness of different approaches to fraud detection in banking. Traditional SIEM systems offer a structured and reliable framework for monitoring and analyzing security events, making them an essential component of cybersecurity infrastructure (Sarker, Kayes, et al., 2020). However, their reliance on predefined rules limits their ability to detect novel and adaptive threats. AI-enhanced SOC operations provide a more advanced approach by leveraging machine learning and data analytics to identify patterns and anomalies in real time. This capability enables organizations to detect previously unknown threats and respond proactively, reducing the risk of financial loss and reputational damage (Bisht et al., 2022). The integration of AI also supports the automation of routine tasks, improving efficiency and allowing security analysts to focus on more complex issues. The comparison between these two approaches highlights the strengths and limitations of each, providing a basis for understanding how they can be integrated to enhance overall security

(Fatima et al., 2020; Islam & Aditya, 2023; Istiaq & Binte, 2023). The combination of traditional and AI-driven methods may offer a balanced approach, leveraging the reliability of rule-based systems and the adaptability of intelligent analytics.

The global landscape of banking cybersecurity is characterized by rapid technological advancements, increasing regulatory requirements, and the growing complexity of cyber threats. AI-enhanced SOC operations play a critical role in addressing these challenges by providing advanced capabilities for detecting and mitigating deepfake and synthetic fraud (Md, 2023; Rojek et al., 2023; Khatun & Zakia, 2023). The international significance of this topic is underscored by the interconnected nature of financial systems, where cyber threats can have far-reaching implications across borders and industries. The adoption of AI in cybersecurity reflects the need to enhance resilience and ensure the integrity of financial operations in an increasingly digital world (Begum & Kaniz, 2024; Djenna et al., 2023; Hisham & Nahar, 2024). Research conducted between 2018 and 2026 has highlighted the importance of integrating advanced technologies into security frameworks, emphasizing the role of AI in improving threat detection and response. At the same time, challenges related to implementation, governance, and system integration remain important considerations for financial institutions. The increasing prevalence of deepfake and synthetic fraud has further emphasized the need for robust and adaptive security measures (El Hajj & Hammoud, 2023; Ahmed, 2024; Towhidul & Uddin, 2024). This study is situated within this evolving context, focusing on the comparative analysis of AI-enhanced SOC operations and traditional SIEM systems in the banking sector.

The primary objective of this study is to quantitatively examine and compare the effectiveness of AI-enhanced Security Operations Center (SOC) operations with traditional Security Information and Event Management (SIEM) systems in detecting and mitigating deepfake and synthetic fraud within the banking sector between 2018 and 2026. This objective is grounded in the need to evaluate how advanced analytical capabilities, such as machine learning–driven anomaly detection, behavioral profiling, and automated response mechanisms, perform relative to rule-based, signature-driven SIEM frameworks in identifying increasingly sophisticated fraud patterns. The study aims to measure key performance indicators, including detection accuracy, false positive and false negative rates, response time, scalability, and adaptability to evolving threat vectors, particularly those associated with AI-generated content and synthetic identities. A further objective is to assess how AI-enhanced SOC systems process large-scale, high-velocity financial data streams compared to traditional SIEM systems, which often rely on static correlation rules and manual intervention. The research also seeks to analyze the operational efficiency of both approaches by evaluating resource utilization, analyst workload reduction, and automation levels in incident response workflows. In addition, the study aims to investigate the robustness of each system in detecting multimodal fraud scenarios, such as voice, video, and identity manipulation, which are characteristic of deepfake-enabled attacks. By employing a comparative quantitative framework, the research intends to generate empirical evidence on whether AI integration significantly enhances fraud detection capabilities in real-world banking environments. The objective further extends to identifying performance gaps, limitations, and contextual conditions under which each system performs optimally, thereby providing a structured basis for evaluating technological advancements in cybersecurity operations. Through this comprehensive comparison, the study seeks to establish measurable benchmarks that define the relative effectiveness of AI-enhanced SOC operations and traditional SIEM systems in addressing the complexities of modern financial fraud.

LITERATURE REVIEW

The literature review section establishes a structured and quantitative understanding of the evolution, capabilities, and performance of AI-enhanced Security Operations Center (SOC) operations in comparison with traditional Security Information and Event Management (SIEM) systems within the banking sector, particularly in the context of deepfake and synthetic fraud detection between 2018 and 2026. SOC environments are fundamentally designed to provide centralized monitoring, detection, and response to cybersecurity threats, while SIEM systems have historically served as the core technological backbone supporting these operations through log aggregation, rule-based correlation, and alert generation (Saraiva & Mateus-Coelho, 2022). Over time, the increasing complexity, volume, and velocity of financial data have exposed limitations in traditional SIEM systems, particularly in handling novel, adaptive, and AI-driven threats. This has led to the emergence of AI-enhanced SOC operations,

which integrate machine learning algorithms, behavioral analytics, and automated response mechanisms to improve detection accuracy and operational efficiency. The growing prevalence of deepfake and synthetic fraud introduces a new dimension to cybersecurity challenges in banking, requiring advanced detection capabilities that extend beyond conventional rule-based systems. Deepfake fraud involves the use of AI-generated media to impersonate individuals, while synthetic identity fraud combines real and fabricated data to create new identities capable of bypassing traditional verification systems. These threats are characterized by their dynamic and evolving nature, making them difficult to detect using static rules and predefined signatures (Berdibayev et al., 2021). As a result, the literature increasingly focuses on AI-driven detection models that leverage large-scale data analysis, anomaly detection, and predictive analytics to identify fraudulent activities in real time. This literature review synthesizes research across multiple domains, including SOC architecture, AI-driven cybersecurity frameworks, deepfake detection technologies, and SIEM-based systems, with a strong emphasis on quantitative performance evaluation. Key metrics such as detection accuracy, false-positive and false-negative rates, mean time to detect (MTTD), mean time to respond (MTTR), and system scalability are central to understanding the comparative effectiveness of these approaches. The review also examines the operational efficiency of AI-enhanced SOC systems in terms of automation levels, data processing capacity, and reduction in analyst workload (Podzins & Romanovs, 2019). By integrating findings from studies conducted between 2018 and 2026, this section provides a comprehensive and data-driven foundation for analyzing how AI-enhanced SOC operations outperform or complement traditional SIEM systems in detecting deepfake and synthetic fraud within banking environments.

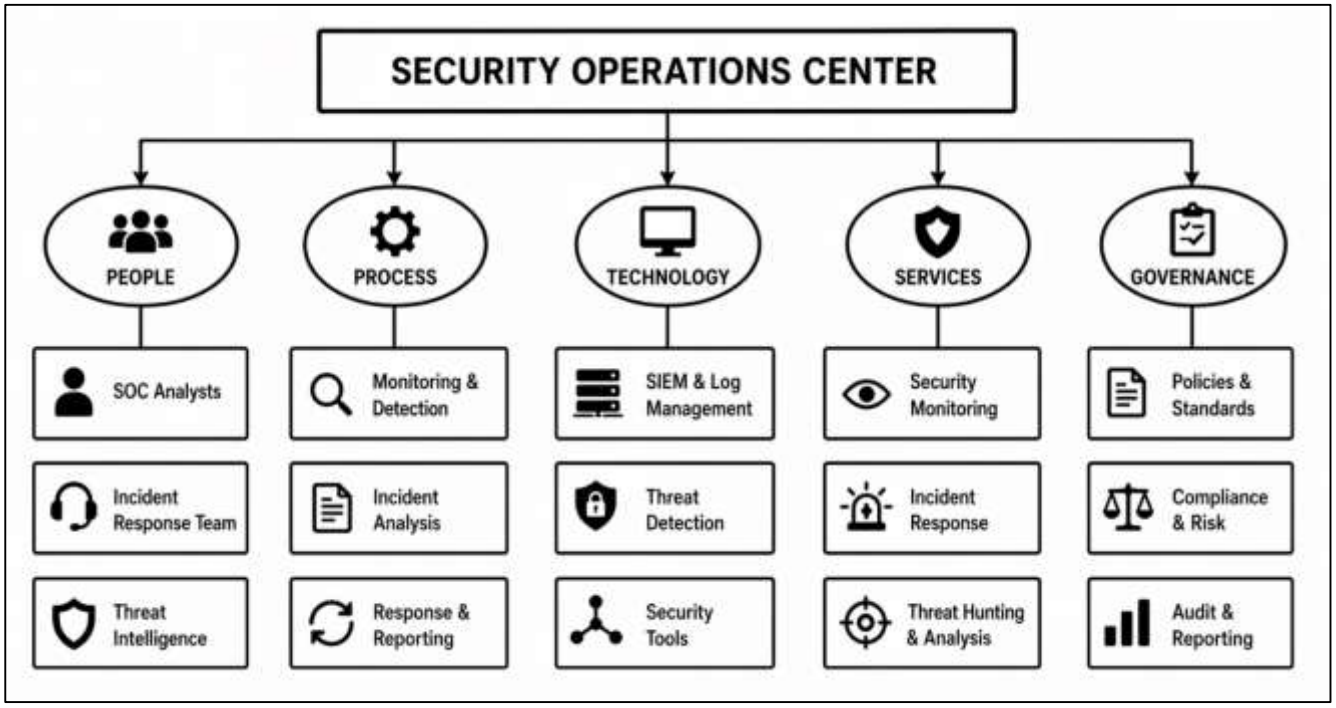
Conceptual Foundations of SOC and SIEM Systems

Security Operations Centers (SOCs) are defined as centralized organizational units responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity threats across enterprise environments, particularly in highly regulated sectors such as banking. Within financial institutions, SOCs integrate people, processes, and technologies to ensure the confidentiality, integrity, and availability of critical financial data and transaction systems (Vielberth et al., 2020). The functional components of a SOC typically include threat intelligence platforms, incident response teams, security monitoring tools, forensic analysis capabilities, and governance frameworks that align with regulatory standards. In banking environments, SOCs operate under stringent compliance requirements, which necessitate real-time visibility into network activities, user behavior, and transaction flows. Studies conducted over the past decade consistently describe SOCs as multi-layered systems that combine human expertise with automated tools to manage complex security events. The increasing digitization of banking services, including mobile banking, online payments, and cross-border financial operations, has amplified the importance of SOCs as the first line of defense against cyber threats (Bryant & Saiedian, 2020). Empirical research highlights that SOC effectiveness is often measured through operational metrics such as incident detection speed, response coordination efficiency, and the ability to handle high volumes of security events. The literature further emphasizes that SOC maturity levels vary across institutions, with advanced SOCs incorporating automation and analytics, while traditional setups rely heavily on manual processes. This variation influences the ability of banking institutions to detect sophisticated fraud schemes, including those involving synthetic identities and manipulated digital content (Orsós et al., 2022; Rajib, 2024; Zakia & Khatun, 2024). The conceptual foundation of SOCs therefore reflects a dynamic interplay between technological infrastructure and organizational capability, where continuous improvement in monitoring and response mechanisms is essential for maintaining financial system resilience.

Traditional Security Information and Event Management (SIEM) systems form the technological backbone of SOC operations by providing centralized log collection, event correlation, and alert generation capabilities (Shahjee & Ware, 2022). SIEM systems are structured around core components that include data ingestion pipelines, storage repositories, correlation engines, and visualization dashboards. These systems collect logs from diverse sources such as servers, network devices, applications, and user endpoints, enabling a consolidated view of security events across the enterprise. The workflow of a typical SIEM system begins with data collection, followed by normalization and enrichment processes, after which correlation rules are applied to identify patterns indicative of

potential threats. Alerts generated through this process are then forwarded to SOC analysts for investigation and response (Albert, 2025; Anick, 2025; Doynikova et al., 2020). Quantitative studies have shown that SIEM systems are capable of processing large volumes of data, often measured in thousands to millions of events per second, depending on system configuration and infrastructure capacity. However, the efficiency of these systems is influenced by factors such as correlation rule complexity, data latency, and storage limitations. Research also indicates that SIEM workflows are inherently reactive, relying on predefined rules that detect known threat patterns rather than adaptive anomalies. This structural characteristic has been widely discussed in the literature as a key limitation in addressing emerging cyber threats. Despite these constraints, SIEM systems remain essential for compliance reporting, audit trails, and baseline security monitoring in banking environments (Dimitrov et al., 2021). The literature consistently portrays SIEM as a foundational yet evolving technology that requires integration with advanced analytics to meet the demands of modern cybersecurity challenges.

Figure 3: SOC Framework for Banking Security



Quantitative performance metrics play a critical role in evaluating the effectiveness of SOC and SIEM systems, providing measurable indicators of operational efficiency and threat detection capability. Among the most commonly analyzed metrics are event ingestion rate, log correlation latency, and alert frequency (Hasan, 2025; Ashfaq & Ashraful, 2025; Villalón-Huerta et al., 2022). Event ingestion rate refers to the volume of security data processed by the system within a given time frame, often reflecting the scalability and throughput capacity of the infrastructure. Studies indicate that high-performing SIEM systems can ingest vast quantities of log data in real time, yet the ability to maintain processing speed without compromising accuracy remains a persistent challenge (Murad, 2025; Shamsul, 2025). Log correlation latency measures the time taken to analyze and correlate incoming data to generate actionable alerts, with lower latency being indicative of faster detection capabilities. Research findings suggest that latency increases significantly as data volume and rule complexity grow, affecting the timeliness of incident detection (Arfaoui et al., 2023; Shamsul & Morshedul, 2025; Bhuya, 2025). Alert frequency, another critical metric, reflects the number of alerts generated within a specific period and is closely associated with system sensitivity and rule configuration. High alert frequency is often linked to increased false positives, which can overwhelm SOC analysts and reduce overall efficiency. Empirical studies across multiple banking institutions reveal that excessive alert volumes contribute to analyst fatigue and decreased response accuracy. Additional metrics such as incident resolution time,

system uptime, and data processing efficiency are also frequently used to assess performance (Vielberth et al., 2021). The literature underscores the importance of balancing these metrics to optimize system performance, as improvements in one area may lead to trade-offs in another. This quantitative perspective provides a comprehensive framework for understanding the operational strengths and limitations of traditional SIEM-supported SOC environments.

Historical performance benchmarks of SIEM systems from 2018 to 2026 reveal a pattern of incremental improvements alongside persistent operational challenges. Early studies in this period highlight the ability of SIEM systems to provide centralized visibility and support regulatory compliance, particularly in detecting known threats and maintaining audit logs (KHetsuriani et al., 2023). Over time, enhancements in data processing capabilities and integration with cloud-based infrastructures have improved scalability and accessibility. However, the literature consistently identifies limitations related to false-positive rates, alert fatigue, and manual investigation time. False positives occur when benign activities are incorrectly flagged as threats, leading to unnecessary investigations and resource expenditure. Quantitative analyses indicate that false-positive rates in traditional SIEM systems can be substantial, often accounting for a majority of generated alerts (Vielberth et al., 2019). This issue contributes directly to alert fatigue, a phenomenon where analysts become desensitized to frequent alerts, potentially overlooking critical incidents. Studies further reveal that the ratio of actionable alerts to total alerts remains low in many SOC environments, highlighting inefficiencies in rule-based detection mechanisms. Manual investigation time is another significant limitation, as analysts are required to review alerts, correlate information, and determine appropriate responses, often under time constraints. Research findings show that prolonged investigation times can delay incident response and increase the risk of successful cyber attacks (Hata et al., 2023). Despite ongoing improvements in system architecture and data processing, these challenges remain prevalent across the literature, emphasizing the need for more advanced and adaptive approaches to cybersecurity. The historical analysis of SIEM performance thus provides critical insights into the structural constraints of traditional SOC operations and sets the foundation for comparative evaluation with emerging AI-enhanced systems.

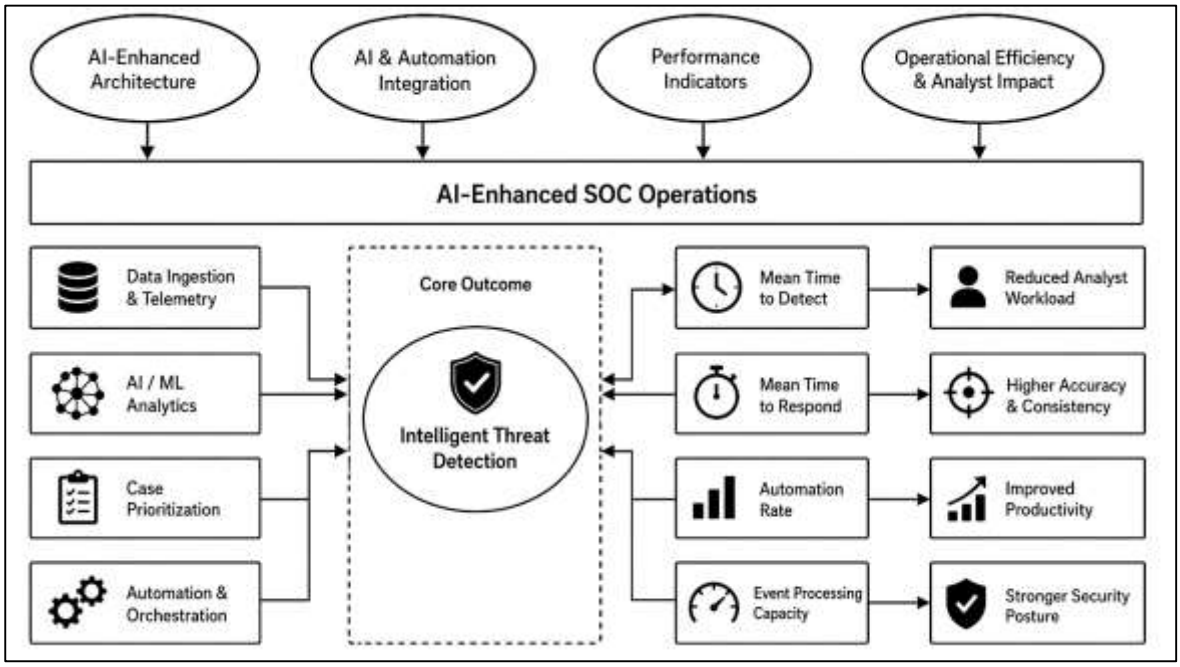
AI-Enhanced SOC Operations

The evolution toward AI-enhanced Security Operations Center (SOC) operations reflects a major shift in cybersecurity management from log-centered monitoring to intelligent, adaptive, and highly automated detection ecosystems (Shi et al., 2023). In the banking sector, AI-driven SOC systems are generally defined as advanced security environments that combine real-time telemetry collection, behavioral analytics, machine learning-based threat classification, deep learning-assisted anomaly recognition, and orchestration tools that support rapid response actions. Unlike conventional SOC models that depend heavily on predefined signatures and analyst-driven triage, AI-driven SOC architecture is built around continuous data learning, contextual correlation, and autonomous support functions. The architecture commonly includes data ingestion layers, feature engineering modules, model inference engines, case prioritization systems, and orchestration platforms that connect detection with remediation workflows. This structural transition emerged as financial institutions began facing attack environments characterized by large-scale digital transactions, omnichannel banking activity, third-party integrations, and increasingly sophisticated fraud tactics. Literature on SOC modernization consistently portrays AI-enhanced operations as a response to the limitations of static security monitoring frameworks, particularly in environments where security alerts are generated across endpoints, identity systems, networks, cloud infrastructure, mobile applications, and transaction platforms at high frequency (Y. Zhu et al., 2023). In banking, this architecture has special relevance because fraud detection requires not only system-level observation but also contextual interpretation of user behavior, device patterns, transaction timing, authentication anomalies, and account activity sequencing. AI-enhanced SOC systems therefore extend beyond infrastructure monitoring and move toward a layered model of risk interpretation. This evolution also represents an organizational change in which cybersecurity operations become less dependent on manual filtering and more dependent on model-assisted prioritization. The literature describes this movement as a progression from reactive monitoring toward intelligent operational resilience, where systems are trained to recognize hidden relationships among events that would be difficult to identify through

static rules alone (Rosa, 2022). As a result, AI-driven SOC systems are increasingly framed in the literature as operational platforms that unify analytics, automation, and decision support to improve the speed, depth, and accuracy of security investigations in banking environments.

A major theme in the literature on AI-enhanced SOC operations is the integration of machine learning, deep learning, and automation tools into the core security workflow. Machine learning contributes to SOC modernization by enabling systems to classify threats, identify anomalies, rank suspicious events, and learn from historical incident data (Damoah et al., 2021). Deep learning extends this capability by supporting pattern recognition across more complex and higher-dimensional datasets, such as user behavior sequences, transaction flows, voice signals, facial data, and multimodal fraud indicators. In banking contexts, these capabilities are particularly valuable because cyber threats and fraud events rarely appear as isolated technical signatures. Instead, they emerge through subtle irregularities across multiple layers of activity, including login behavior, transaction timing, biometric mismatches, identity verification anomalies, and synthetic media artifacts. Automation tools complement these analytical capabilities by performing repetitive operational tasks such as alert enrichment, ticket creation, threat scoring, evidence collection, response playbook execution, and incident routing. The literature consistently emphasizes that the combined effect of learning algorithms and orchestration tools is what distinguishes AI-enhanced SOC systems from earlier generations of automated monitoring (Bozzano et al., 2022). Rather than functioning as independent software additions, machine learning models, deep learning engines, and automated workflows are integrated into a unified pipeline in which detection, triage, prioritization, and response are connected. This integrated model is important in banking because operational delays can increase fraud exposure and magnify financial loss. Studies on AI-driven SOC environments frequently note that automation enables analysts to focus on higher-complexity cases rather than repetitive alert validation. The literature also shows that deep learning tools are increasingly applied to fraud scenarios involving synthetic identities, manipulated documents, voice cloning attempts, and account takeover patterns, especially where static rule thresholds fail to capture the evolving nature of the threat (Behrooz et al., 2023). In practical terms, the integration of these tools transforms the SOC from a passive recipient of alerts into a semi-autonomous analytic environment capable of continuously refining threat visibility. This shift is not only technological but procedural, as it changes how investigations are initiated, how evidence is assembled, and how analysts allocate time and cognitive effort across the alert landscape.

Figure 4: AI-Enhanced SOC Operational Framework



Quantitative indicators occupy a central place in the literature examining the effectiveness of AI-enhanced SOC operations, especially Mean Time to Detect, Mean Time to Respond, automation rate, and event processing capacity. These indicators are used to demonstrate whether AI integration translates into measurable operational gains when compared with traditional security monitoring approaches (Zhu et al., 2023). Mean Time to Detect is commonly used to assess how quickly a system recognizes a suspicious event after its occurrence, while Mean Time to Respond captures the interval between detection and implementation of a containment or remediation action. In banking environments, these measures are particularly important because the speed of recognizing fraudulent behavior often determines whether a financial loss can be prevented, contained, or recovered. Literature on AI-enhanced SOC performance repeatedly reports that intelligent analytics shorten both detection and response cycles by correlating signals at machine speed and routing high-priority incidents to automated or analyst-supported workflows. Automation rate is another widely discussed metric, referring to the percentage of operational tasks executed without direct manual intervention. This includes enrichment, prioritization, duplicate suppression, case forwarding, and playbook-based response actions. Higher automation rates are associated in the literature with improved throughput, reduced backlog, and more consistent handling of repeatable security scenarios (Chen et al., 2023). Event processing capacity, often discussed in terms of events per second, is another critical indicator in modern banking SOC environments because institutions generate very high volumes of telemetry from transactions, devices, applications, cloud services, identity systems, and customer-facing platforms. Literature comparing AI-enhanced systems with more traditional monitoring structures suggests that intelligent architectures are more effective at processing high event volumes while still preserving contextual prioritization. This matters because raw ingestion speed alone has limited value if alert quality deteriorates under scale (Wang et al., 2021). The literature therefore treats these indicators as interconnected rather than isolated. Faster detection is meaningful when supported by sufficient event processing capacity, and high automation is valuable when it contributes to faster, more accurate response actions. Altogether, these quantitative indicators form the empirical foundation for evaluating AI-enhanced SOC maturity and provide a consistent basis for understanding how intelligent operational models improve security performance in banking.

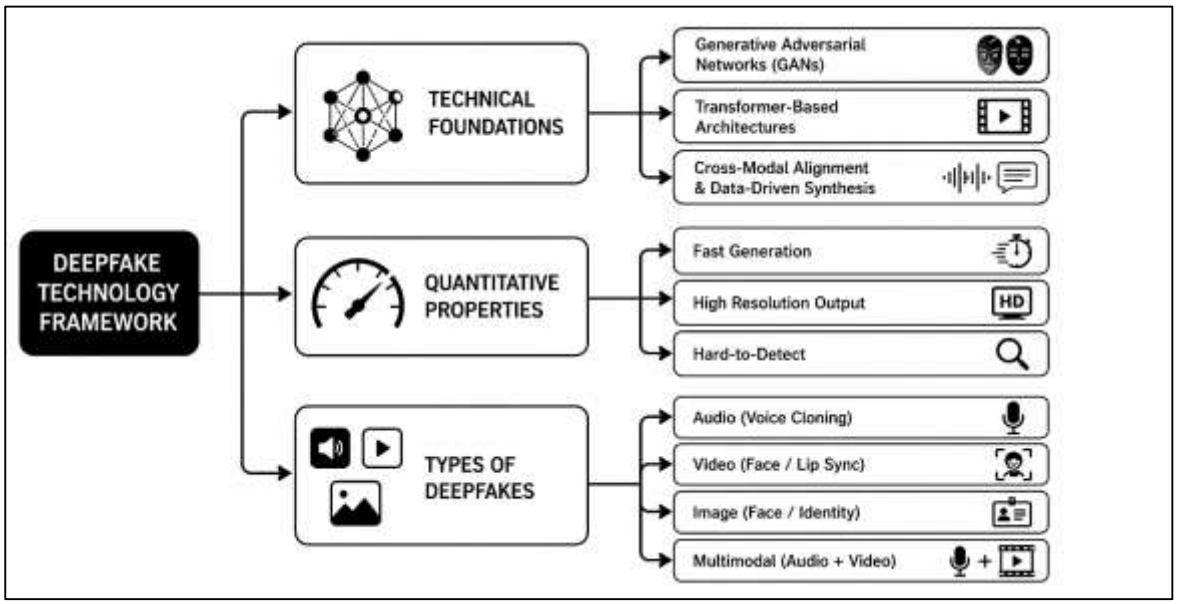
Another strongly synthesized theme in the literature is the reduction in analyst workload and the broader increase in operational efficiency associated with AI-enhanced SOC adoption. Traditional SOC environments often require analysts to manually review large alert queues, correlate fragmented evidence, validate event severity, investigate false positives, and coordinate responses across multiple tools. This workflow is time intensive and cognitively demanding, especially in banking institutions that process continuous streams of sensitive activity and face regulatory pressure for timely incident handling (Helkala et al., 2022). The literature describes analyst fatigue as a structural weakness of conventional SOC operations, particularly where alert volumes are high and many notifications are repetitive, low-confidence, or non-actionable. AI-enhanced SOC systems address this problem by automating early-stage triage, suppressing redundant alerts, enriching cases with contextual data, and ranking incidents according to learned risk patterns. This directly reduces the volume of manual review required at the analyst level. A recurring finding across the literature is that operational efficiency improves when AI is used to convert raw security data into prioritized investigative pathways rather than undifferentiated alert streams. In banking environments, this efficiency gain extends beyond analyst comfort and becomes a strategic matter because delayed review can permit fraud escalation, compromise customer trust, and disrupt transaction integrity (Stecuła et al., 2023). AI-enhanced systems also improve workflow consistency by standardizing repetitive decisions that would otherwise vary across analyst teams. This has important implications for large SOC operations where staffing levels, skill differences, and shift-based turnover can affect investigative quality. Literature further suggests that when analysts are relieved of routine triage and evidence gathering, they can devote more time to higher-value tasks such as fraud pattern interpretation, escalation decisions, cross-case synthesis, and incident strategy development. Operational efficiency is therefore not simply measured by speed, but by the redistribution of human expertise toward more complex and judgment-intensive activities (Oliveri et al., 2022). The literature consistently frames this shift as one of the defining advantages of AI-enhanced SOC operations, especially in financial institutions where scale,

precision, and timeliness must coexist. In this sense, the movement toward AI-enhanced SOCs is understood not only as a technological upgrade but also as a restructuring of security labor, analytical focus, and institutional response capability.

Technical Foundations of Deepfake Technology

Deepfake technology is grounded in a set of computational models designed to generate highly realistic synthetic media by learning patterns from authentic human data. The literature consistently identifies generative adversarial networks and transformer-based architectures as the two most influential foundations in the development of modern deepfakes (Kwok & Koh, 2021). Generative adversarial networks introduced a competitive learning structure in which one model generates synthetic content and another evaluates whether the output appears authentic, thereby improving realism through repeated optimization. This framework became central to the early expansion of deepfake systems because it enabled image synthesis, face swapping, facial reenactment, and identity mimicry with increasingly convincing visual quality. Transformer architectures later expanded the technical scope of deepfakes by enabling stronger temporal consistency, more coherent sequence generation, and better contextual understanding across audio, text, and video streams. In the literature, transformers are often associated with improved continuity in facial expressions, lip movement, speech synchronization, and cross-modal alignment, especially in systems that generate voice and video simultaneously. The technical significance of these models lies in their ability to learn large-scale data representations rather than rely on hard-coded manipulation rules (Sareen, 2022). This data-driven structure made deepfake systems more scalable, more adaptive, and more accessible to both research and criminal misuse. Studies across the review period describe a transition from earlier low-resolution, artifact-heavy manipulations to high-fidelity synthetic outputs that preserve identity cues, emotional expression, and realistic motion patterns. The technical foundations are therefore not limited to one algorithmic family but reflect an expanding architecture of synthesis models, enhancement layers, data preprocessing methods, and post-generation refinement tools. The literature also indicates that improvements in computing power, open-source model availability, and large multimedia training datasets contributed substantially to the rapid growth of these systems (Laas, 2023). In banking-related threat discussions, these model developments are particularly important because they underpin the ability of attackers to create false customer identities, impersonate executives, fabricate voice authentication samples, and manipulate visual verification processes. The technical literature thus frames deepfake technology as a convergence of machine learning innovation, computational efficiency, and representational realism, all of which have transformed synthetic media from a niche research topic into a high-risk fraud instrument.

Figure 5: Deepfake Detection Technology Framework



The quantitative properties of deepfake systems form a major area of emphasis in the literature because the operational danger of synthetic media is closely linked to how quickly it can be produced, how realistic it appears, and how difficult it is to detect. Generation speed is frequently discussed as a critical marker of technological maturity. Earlier systems required substantial training time and post-processing effort, which limited output frequency and accessibility. Over time, research shows that improvements in hardware acceleration, pretrained models, transfer learning, and optimized generation pipelines significantly reduced the time required to create convincing synthetic content (Shoaib et al., 2023). This increase in speed has direct implications for fraud operations because faster generation enables repeated attack attempts, personalized targeting, and rapid adaptation to verification demands. Resolution quality is another widely discussed property, particularly in image and video deepfakes. Higher resolution outputs reduce visible artifacts, improve facial detail, preserve texture consistency, and support more convincing impersonation across digital channels. The literature commonly describes quality improvement as a function of better training data, stronger model architectures, and more effective enhancement stages that refine edges, lighting, and motion continuity (Gaur et al., 2022). Another important quantitative feature in the literature is detection complexity, which refers to the degree of difficulty involved in distinguishing synthetic media from authentic material. Detection complexity increases when synthetic content shows fewer visual distortions, stronger temporal consistency, better audio synchronization, and more natural human movement. Studies examining forensic detection methods often describe an ongoing escalation between generation quality and detection difficulty, with manipulations becoming harder to identify as models improve. This difficulty is especially relevant in banking because security systems often rely on rapid verification processes rather than long-form forensic examination. The literature shows that when synthetic media can be generated quickly, at high quality, and with limited obvious artifacts, traditional verification workflows become more vulnerable to misuse. Quantitative evaluation in this area is therefore not only about model performance in a technical sense but also about operational risk in real-world environments (Pashentsev, 2023). Across the review period, the literature consistently links improvements in generation speed and output quality with increased detection difficulty, creating a technical trajectory in which the realism of deepfakes has advanced alongside their potential for criminal exploitation.

The literature classifies deepfakes into several major types, most commonly audio, video, image, and multimodal forms, each with distinct technical characteristics and fraud implications. Audio deepfakes involve synthetic voice generation or voice cloning that imitates tone, cadence, accent, and speaking style (Pawelec, 2022). These systems are particularly threatening in banking because voice verification is often used in call center authentication, transaction confirmation, and executive communication channels. Video deepfakes typically involve facial reenactment, lip synchronization, or full-face replacement, allowing attackers to fabricate visual evidence of identity or authority. In banking environments, such outputs can be used to deceive employees during video-based approval processes or to bypass remote identity checks. Image deepfakes include static identity manipulations, forged profile photographs, fake identification materials, and synthetic face generation used for account opening or documentation fraud. Multimodal deepfakes combine two or more forms, such as synchronized voice and video, to create highly persuasive impersonation attempts (De Ruiter, 2021). The literature repeatedly emphasizes that multimodal systems present greater fraud potential because they mimic multiple dimensions of human authenticity at once. This classification matters because each type poses different detection challenges and interacts differently with institutional control systems. Audio manipulations may evade telephone verification, visual manipulations may exploit video onboarding, and multimodal manipulations may target high-value transactions requiring combined identity cues. Across the literature, the movement from isolated manipulation formats toward multimodal synthesis is presented as a sign of rising technical sophistication. Research also highlights that the boundaries among categories are becoming less rigid as unified models begin to generate integrated media outputs rather than separate artifacts (Whyte, 2020a). This trend increases the operational burden on fraud detection systems because defense mechanisms must evaluate not only whether a face looks real or a voice sounds real, but whether both align consistently within a broader behavioral and contextual frame. The literature therefore treats deepfake typology as more than a

descriptive classification; it is a practical framework for understanding risk exposure, detection complexity, and attack strategy. In the context of banking fraud, this typology helps explain why deepfake threats have become harder to contain, as institutions must now secure multiple modes of identity verification against increasingly coordinated synthetic manipulation.

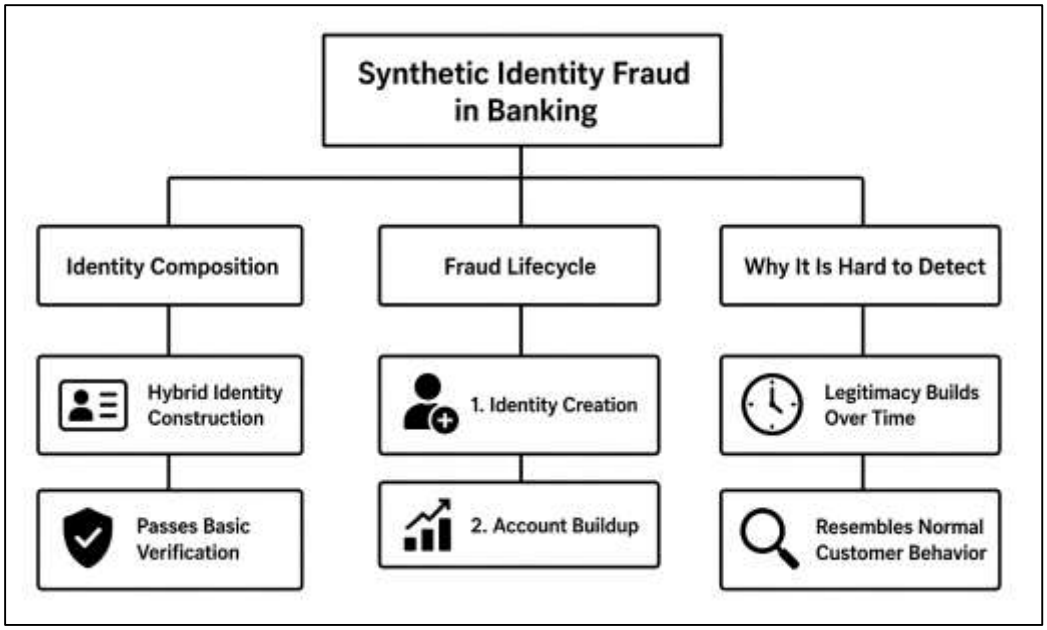
Synthetic Identity Fraud in Banking

Synthetic identity fraud in banking is widely defined in the literature as a form of financial deception in which a fraudster constructs a new identity by combining authentic and fabricated personal information to create an apparently legitimate customer profile (Benalcazar et al., 2023). Unlike traditional identity theft, which depends on fully stealing and misusing the credentials of an existing person, synthetic identity fraud operates through hybrid identity construction, often involving a real identifier such as a social security number, national identification number, tax number, phone number, or address element that is merged with invented names, dates of birth, employment records, and contact details. Literature in fraud analytics consistently characterizes synthetic identities as structurally deceptive because they do not initially resemble classic stolen identities or obviously fictitious accounts. Instead, they occupy an ambiguous zone between authenticity and fabrication, which makes them difficult for conventional banking controls to classify. In banking environments, this composition often allows the identity to pass basic onboarding checks, especially where verification systems emphasize document presence, rule-based consistency, or limited-file credit history rather than deeper behavioral validation. Studies across financial crime, digital identity management, and credit risk monitoring describe synthetic identity fraud as particularly dangerous because it exploits the architecture of modern banking itself, including remote onboarding, digital lending, automated customer scoring, and fragmented identity verification systems (Beju & Făt, 2023). The literature also notes that synthetic identities may be created from vulnerable populations' identifiers, including minors, the elderly, migrants, or persons with limited credit activity, because these records can remain unused long enough to avoid rapid detection. In some cases, fraudsters create entirely fresh profiles through coordinated manipulation of phone records, email accounts, device histories, and fabricated supporting documents. This makes synthetic identity fraud not merely a case of fraudulent application behavior, but a layered process of identity engineering. Banking studies further emphasize that the composition of synthetic identities has become more sophisticated as digital ecosystems have expanded, allowing fraud actors to support fake personas through social traces, account activity, and transactional patterns that mimic legitimate customer behavior (Oliveira et al., 2020). As a result, the literature consistently presents synthetic identity fraud as a uniquely adaptive and institutionally embedded threat that differs from ordinary impersonation because it is designed to grow inside the banking system rather than simply attack it from the outside.

The fraud lifecycle of synthetic identity activity is a central theme in the literature, and most studies organize it into three major phases: identity creation, account buildup, and financial extraction. During the identity creation stage, fraudsters assemble the synthetic profile using a mix of genuine and invented information, ensuring sufficient consistency to satisfy entry-level verification checks. The literature shows that this first stage often relies on weaknesses in customer due diligence systems, fragmented databases, inconsistent identity standards, and automated approvals that reward surface-level legitimacy. Once the identity is accepted, the account buildup phase begins (Mytnyk et al., 2023). This stage is especially important because it distinguishes synthetic identity fraud from more immediate fraud types. Instead of extracting value immediately, the fraudster cultivates the identity over time by opening accounts, making small transactions, repaying balances, establishing credit lines, or interacting with digital banking systems in ways that simulate authentic customer development. Studies frequently describe this stage as one of strategic patience, where the objective is to improve the identity's credibility, increase creditworthiness, and reduce suspicion through apparently normal financial behavior. In banking literature, this maturing phase is often associated with "grooming" or "aging" the identity, because the fraud becomes stronger as the account accumulates legitimacy signals (Mayer et al., 2020). The final stage, financial extraction, occurs when the synthetic identity has achieved sufficient trust within the institution. At this point, fraudsters maximize withdrawals, exploit credit extensions, conduct bust-out activity, default intentionally, or redirect funds through layered transactions. Research indicates that this final phase often causes the largest losses because institutions

treat the customer as a known account holder until the behavior becomes clearly abnormal. The lifecycle perspective is important because it demonstrates that synthetic identity fraud is not an isolated fraudulent act but a longitudinal process that exploits time, trust, and institutional scoring logic. The literature repeatedly emphasizes that banks struggle not only because the identity appears legitimate at the start, but because each stage reinforces the next. Identity creation gains credibility through account buildup, and account buildup enables larger-scale extraction (Langevin et al., 2022). This multi-stage structure explains why synthetic identity fraud is harder to detect than many traditional fraud forms, since the fraud is intentionally designed to resemble ordinary customer progression over an extended period.

Figure 6: Synthetic Identity Fraud Lifecycle Framework

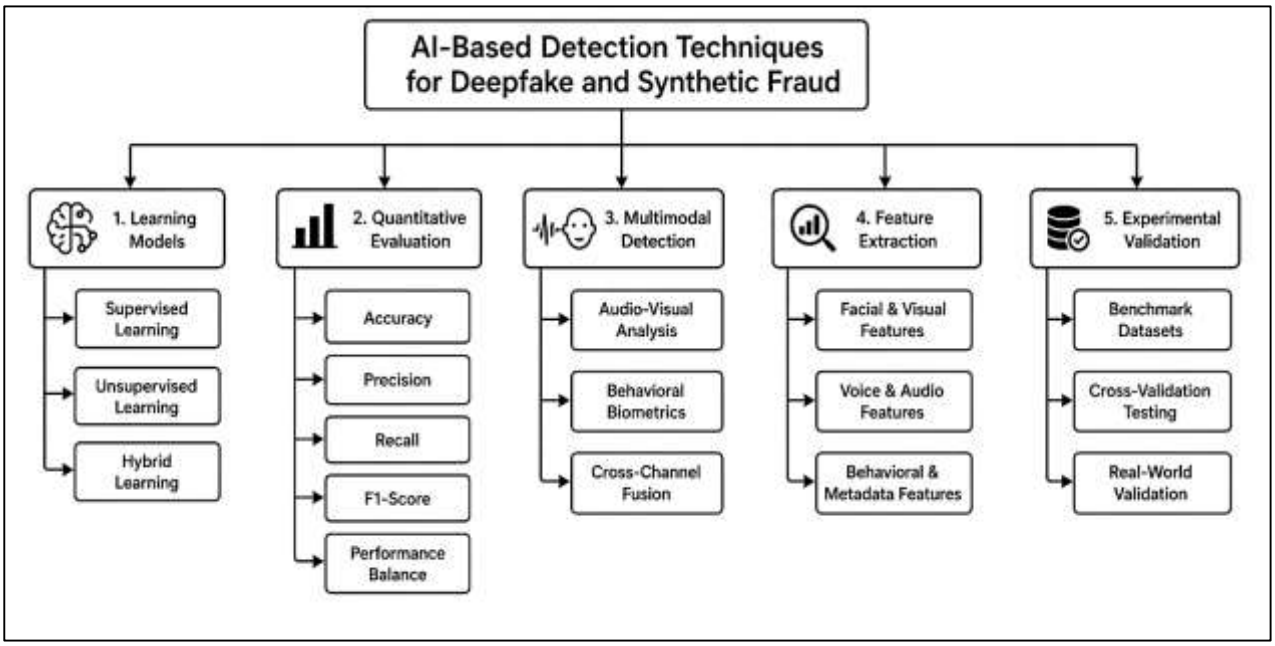


AI-Based Detection Techniques for Deepfake and Synthetic Fraud

AI-based detection techniques for deepfake and synthetic fraud have developed into a major stream of cybersecurity and financial fraud literature, particularly as banking institutions confront increasingly adaptive forms of identity manipulation and synthetic media abuse. The literature commonly organizes these techniques into supervised, unsupervised, and hybrid learning models, each of which reflects a different logic of fraud recognition (Cross, 2022). Supervised learning models rely on labeled datasets in which instances of authentic and fraudulent behavior are already categorized, allowing algorithms to learn patterns associated with known manipulation strategies. In deepfake detection, supervised systems are frequently used to distinguish genuine media from altered voice, image, or video samples by learning discriminative patterns from previously identified manipulations. In synthetic fraud detection, supervised models are applied to transaction histories, onboarding records, customer profiles, device traces, and behavioral patterns to classify whether an account or event is likely fraudulent. Unsupervised learning models, by contrast, do not depend on predefined labels and are therefore emphasized in the literature as valuable for discovering previously unknown fraud patterns, especially when attackers continuously evolve their techniques (Garde et al., 2022). These models identify deviations from expected behavior, cluster unusual activity, and surface anomalies that may indicate synthetic identity growth, account misuse, or media manipulation that has not yet been formally categorized. Hybrid models combine both strategies and are often described as especially effective in fraud-heavy banking environments because they support detection of both known and emerging threats. Across the literature, the appeal of hybrid systems lies in their ability to incorporate established fraud indicators while remaining sensitive to unusual behavior that falls outside previously labeled categories. This is particularly important in the context of deepfake and synthetic fraud, where

threat actors frequently alter methods in response to institutional controls. The literature also frames these learning models as operating within broader banking security ecosystems that include event monitoring, identity verification, case management, and analyst oversight. Rather than treating supervised, unsupervised, and hybrid learning as isolated technical categories, the literature presents them as complementary approaches that reflect the layered complexity of modern fraud detection (Lyu, 2022). In this regard, AI-based detection is not simply an algorithmic substitute for traditional controls, but a methodological shift toward dynamic, data-driven interpretation of fraudulent activity that is better aligned with the speed, variability, and ambiguity of digital banking threats.

Figure 7: AI Fraud Detection Framework



Quantitative evaluation occupies a central role in the literature on AI-based fraud detection because the credibility of any detection model depends on measurable evidence of performance under realistic conditions. Studies consistently assess AI systems through indicators such as accuracy, precision, recall, and F1-score, using these metrics to evaluate whether a model can correctly identify fraudulent instances while minimizing incorrect classifications (Gautam et al., 2023). In the literature, accuracy is often used as an initial indicator of overall detection capability, yet many scholars caution that high accuracy alone can be misleading in fraud settings where legitimate cases vastly outnumber fraudulent ones. As a result, greater emphasis is frequently placed on precision and recall. Precision is discussed as particularly important in banking because it reflects the extent to which flagged cases are truly fraudulent, which has implications for operational efficiency and customer friction. A model with low precision may overwhelm analysts with false alarms and create unnecessary interventions for legitimate customers (Mukta et al., 2023). Recall is equally emphasized because it reflects the model's ability to capture actual fraud cases, and weak recall in banking environments can lead to missed attacks, financial loss, and institutional exposure. The literature often treats F1-score as a useful balance between precision and recall, especially when evaluating models in imbalanced datasets that resemble real-world fraud distributions. Comparative studies regularly show that AI-based systems are judged not only by how often they are correct, but by how effectively they balance sensitivity and selectivity under varying fraud conditions. In deepfake detection research, these metrics are applied to assess how well models distinguish authentic from manipulated audio, video, and image samples. In synthetic fraud studies, the same metrics are used to evaluate classification of suspicious accounts, application records, and transaction behaviors. The literature also connects these quantitative indicators to institutional consequences (Sharma & Kaur, 2021). A model with strong recall but weak precision may impose heavy review burdens on banking analysts, while a model with strong precision but weak recall may miss strategically important fraud events. This is why performance evaluation in the literature is

rarely reduced to a single score. Instead, scholars use a combination of metrics to assess trade-offs, context fit, and operational relevance. The quantitative tradition in this body of research therefore serves not only as a technical reporting framework but also as a mechanism for linking model behavior to banking risk, workload management, and fraud control effectiveness.

A major development in the literature is the rise of multimodal detection approaches, which have become increasingly important as both deepfake and synthetic fraud evolved beyond simple one-channel manipulations. Multimodal detection refers to the use of multiple forms of input data, such as voice, facial movement, transaction behavior, typing patterns, device signals, document structure, and metadata traces, in order to identify fraud more reliably than would be possible through a single source of evidence (Baraheem & Nguyen, 2023). In deepfake research, audio-visual approaches are especially prominent because manipulated media often involve synchronization between speech and facial expression. The literature shows that evaluating visual appearance alone may miss sophisticated edits, while combining voice patterns with lip movement, timing consistency, and temporal behavior improves detection robustness. In banking environments, multimodal methods are also extended to behavioral biometrics, which include how a user interacts with systems through gestures, keystroke patterns, mouse dynamics, touchscreen pressure, navigation sequences, and transaction behavior. Scholars in fraud detection argue that synthetic identities and impersonation attacks may replicate static credentials, but they often struggle to reproduce the full behavioral signature of a legitimate user over time (Mubarak et al., 2023). This makes multimodal systems especially attractive in financial services, where authentication and fraud prevention increasingly depend on layered digital interactions rather than single-point identity checks. The literature also emphasizes that multimodal detection is valuable because fraud itself is increasingly multimodal. Synthetic fraud may combine forged documents, manipulated images, false voice interactions, suspicious onboarding patterns, and abnormal transaction behavior into one coordinated attack path. Consequently, models that evaluate only one feature domain are seen as less capable of capturing the broader logic of fraudulent activity. Studies in this field suggest that combining media forensics with behavioral analytics provides stronger resilience against sophisticated attacks, since inconsistencies may emerge across channels even when one modality appears convincing (Raj et al., 2023). The literature therefore presents multimodal detection as both a technical and strategic advancement, one that mirrors the complexity of the fraud environment itself. In banking cybersecurity research, this approach is frequently associated with improved robustness, richer contextual analysis, and better resistance to evasion tactics, making it one of the most significant directions in AI-based deepfake and synthetic fraud detection.

Feature extraction and experimental validation form another core area of the literature, as the success of AI-based detection depends heavily on which signals are captured, how they are represented, and how reliably models are tested. In deepfake detection studies, feature extraction often focuses on facial micro-patterns such as unnatural blinking rhythms, irregular skin texture, inconsistent lighting, boundary distortions, abnormal eye reflections, or subtle mismatches in expression dynamics (Patel et al., 2023). For voice-based fraud detection, the literature frequently highlights features related to voice frequency anomalies, spectral irregularities, prosodic instability, timing distortions, and artifacts in pitch or cadence that may reveal synthetic generation. In synthetic identity fraud research, feature extraction extends into metadata inconsistencies, identity record mismatches, device reuse signals, network anomalies, suspicious document characteristics, transactional irregularities, and cross-channel discrepancies in customer behavior. The literature repeatedly emphasizes that the strength of an AI model depends not only on its architecture but on the relevance and quality of the extracted features, since fraud detection is often won or lost at the stage of signal representation. Experimental validation methods are therefore treated as essential to scientific credibility (Kingra et al., 2023). Benchmark datasets are widely used to train and test models, and the literature discusses their importance in enabling reproducibility, cross-study comparison, and controlled performance evaluation. In deepfake research, benchmark datasets typically include manipulated audio, images, and videos under varying conditions of quality and realism. In synthetic fraud studies, validation datasets may include labeled application records, transaction histories, customer onboarding data, or simulated fraud scenarios built to test account-level detection. Scholars also note important limitations in benchmark reliance, particularly when laboratory datasets fail to capture the messiness of real banking environments or

when manipulated samples do not reflect the sophistication of live fraud attempts. As a result, many studies complement benchmark testing with cross-validation, holdout testing, scenario-based experiments, or institution-specific validation pipelines (Masood et al., 2023). The literature consistently argues that robust evaluation requires both technical control and contextual realism. This is especially important in banking, where the operational value of a detection model depends on how it performs under high data volume, variable fraud tactics, and incomplete information. Altogether, the literature on feature extraction and validation presents AI-based detection as a carefully staged process in which signal selection, data quality, and testing design are just as important as the learning model itself.

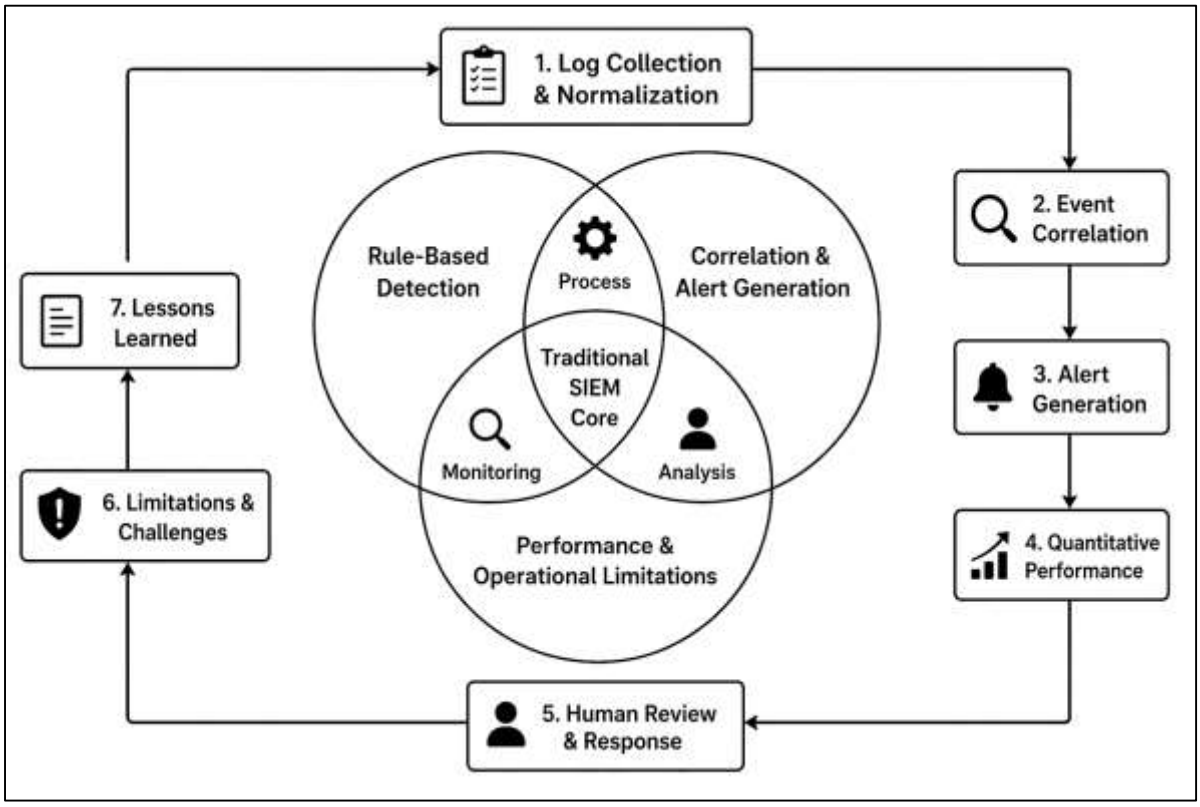
Traditional SIEM-Based Detection Mechanisms

Traditional Security Information and Event Management (SIEM)-based detection mechanisms are widely described in the literature as foundational to modern cybersecurity monitoring, particularly in highly regulated sectors such as banking, where centralized visibility, auditability, and event traceability are essential (López Velásquez et al., 2023). SIEM systems are generally built on rule-based logic and signature detection frameworks, meaning that they rely on predefined conditions, known threat indicators, and codified patterns of suspicious activity to identify potential incidents. In practical terms, these systems ingest logs from firewalls, servers, identity platforms, applications, databases, network devices, endpoints, and transaction environments, then normalize and analyze those records against an established library of detection rules. Banking institutions adopted SIEM technologies extensively because they offered a structured means of consolidating fragmented security data into a central monitoring environment, thereby supporting compliance obligations, internal governance, and incident documentation. The literature consistently portrays rule-based detection as both the main strength and the main structural limitation of traditional SIEM (Tuyishime et al., 2023). Its strength lies in predictability, repeatability, and transparency. A well-designed rule can reliably identify a known attack pattern, suspicious login sequence, privileged access anomaly, or data exfiltration attempt when the event characteristics match prior knowledge. In banking contexts, this model has been especially useful for identifying standard forms of credential abuse, transaction anomalies that cross preconfigured thresholds, and repeated policy violations across user and system activity. Signature detection frameworks add another layer by matching events against previously observed malicious patterns, such as known malware behaviors, blacklisted indicators, suspicious IP addresses, or established fraud signals (Sebbar et al., 2023). The literature often emphasizes that this structure makes SIEM attractive to organizations seeking control, stability, and explainability in security operations. Analysts can inspect the logic behind alerts, compliance officers can map monitoring procedures to regulatory requirements, and administrators can tune rules based on internal risk priorities. At the same time, the literature repeatedly stresses that the conceptual design of traditional SIEM is rooted in prior knowledge, which means it is most effective when malicious behavior resembles something already anticipated by analysts or encoded within the system. This dependence on predefined logic has shaped the historical role of SIEM in banking security, positioning it as a reliable but essentially reactive mechanism for monitoring threats that fit within known behavioral templates.

The operation of traditional SIEM systems depends heavily on correlation rules and alert generation mechanisms, which the literature identifies as the core processes through which raw logs are transformed into actionable security signals. Correlation logic is used to connect events that may appear insignificant when viewed separately but become suspicious when interpreted together across time, source, device, or user behavior. For example, repeated failed login attempts followed by successful privileged access, unusual transaction activity, and abnormal system communications may trigger an alert when processed through a predefined rule set (Majeed et al., 2019). In banking environments, this correlation model has long been valued because threats rarely emerge as single isolated events; rather, they unfold as sequences of actions distributed across applications, identity systems, customer channels, and transaction infrastructure. SIEM systems therefore attempt to reconstruct suspicious narratives through pattern linkage, rule chaining, threshold conditions, and temporal windows. The literature shows that these mechanisms can be effective in controlled and well-understood environments, especially when the threat model is stable and the rules are tuned to institutional risk behavior. Alert generation then occurs once a rule threshold is met, producing a notification for SOC analysts to review, prioritize, and investigate. Many studies emphasize that alert generation is not

merely a technical outcome but an operational event, because it determines how analysts allocate time and how organizations interpret risk exposure (Fuentes-García et al., 2021). In banking security operations, alert volume is often high due to the constant production of logs from payment systems, customer accounts, authentication services, internal networks, fraud controls, and regulatory monitoring tools. The literature repeatedly notes that the quality of correlation logic determines whether this volume becomes manageable intelligence or overwhelming noise. If rules are too broad, alert generation becomes excessive and operationally disruptive. If rules are too narrow, important threats may remain undetected. This tension is central to the literature on SIEM design and performance. Researchers often describe traditional SIEM as an architecture of conditional visibility, meaning that what it detects depends almost entirely on how well its rules have been designed, tuned, and updated. In this sense, alert generation is both the product and the limit of the system (Hasan et al., 2019). It reflects the institution's prior assumptions about risk and translates those assumptions into operational signals, yet it does not inherently reason beyond them. That characteristic explains both the enduring usefulness and the persistent criticism of traditional SIEM-based detection in banking.

Figure 8: Traditional SIEM Detection Framework



Quantitative performance analysis in the literature provides a more detailed understanding of how traditional SIEM-based detection mechanisms function in practice, especially when examined through detection rate, false-positive levels, and alert escalation time. Detection rate is commonly used to assess how many genuine threats a SIEM system successfully identifies within the overall threat landscape (Pitropakis et al., 2019). In banking environments, this metric is important because missed incidents may translate into financial loss, regulatory exposure, account compromise, or prolonged system misuse. The literature generally shows that traditional SIEM performs adequately in identifying known threats and policy-defined anomalies, particularly when rules are carefully aligned with recurring attack patterns or institutional risk thresholds. However, this performance often declines when the environment becomes more dynamic, the threat patterns more subtle, or the event volume more complex. False positives are an even more prominent issue in the literature. A false positive occurs when benign activity is incorrectly classified as suspicious, generating an alert that consumes analyst attention without corresponding to a genuine threat. Studies repeatedly identify false positives as one

of the most persistent operational burdens associated with traditional SIEM systems (Pitropakis et al., 2019). In high-volume banking environments, where legitimate customer behavior can vary widely across devices, geographies, channels, and transaction timing, rigid rules may flag normal variation as risk, thereby inflating alert queues. This leads directly to concerns over alert escalation time, another critical quantitative measure. Alert escalation time refers to how long it takes for an alert to move from initial detection into analyst review, prioritization, and response handling. The literature indicates that when false-positive volume is high, escalation slows because analysts must manually filter large numbers of low-value alerts before they can reach genuinely urgent cases. This backlog effect is especially problematic in banking because time-sensitive fraud scenarios may evolve quickly once initiated (Najafi et al., 2021). The literature frequently connects these metrics to one another rather than treating them in isolation. A higher detection rate is not necessarily beneficial if it is achieved through overly sensitive rules that flood analysts with false alarms, and a manageable false-positive level loses value if escalation remains slow due to process inefficiencies. The quantitative literature therefore presents SIEM performance as a balance problem shaped by tuning quality, infrastructure scale, analyst capacity, and institutional complexity. Traditional SIEM may offer measurable visibility, but the literature consistently shows that this visibility often comes at the cost of operational friction when alert quality and response flow are not carefully controlled.

A major conclusion synthesized across the literature is that traditional SIEM-based detection mechanisms face serious limitations in identifying unknown or adaptive threats and remain heavily dependent on human intervention and manual workflows. These limitations are especially significant in banking, where attack patterns increasingly involve novel fraud sequences, synthetic identities, insider misuse, advanced phishing, credential manipulation, and AI-supported deception that do not always match predefined rules or known signatures (Lee & Huh, 2019). The literature repeatedly argues that traditional SIEM is structurally disadvantaged in such situations because its detection logic is anchored in codified expectation. When malicious behavior departs from those expectations, the system may fail to recognize it as suspicious. Adaptive threats are particularly problematic because they evolve in response to institutional controls, often changing behavior just enough to evade threshold-based or signature-based monitoring. Unknown threats create an even deeper challenge because there may be no rule template available to detect them at all. This explains why many studies characterize traditional SIEM as effective for visibility and compliance but weaker in discovery and adaptation. The second major limitation concerns operational dependence on human analysts. Once alerts are generated, traditional SIEM workflows generally require manual triage, contextual review, evidence gathering, prioritization, escalation, and decision-making (Sen et al., 2021). Analysts must determine whether the alert is meaningful, whether it corresponds to a broader incident, and what response is appropriate. In banking SOCs, where alerts may span customer behavior, payment anomalies, network activity, authentication logs, and fraud indicators, this manual burden can be substantial. The literature frequently links this dependence on human intervention to analyst fatigue, inconsistency in case handling, slower response times, and greater exposure to backlog accumulation. Manual workflows also create variability, since outcomes may differ depending on analyst experience, shift timing, institutional procedures, and competing workload pressures. Traditional SIEM thus becomes not only a technical system but a labor-intensive operational environment that relies on human judgment to convert alerts into meaningful action. The literature does not dismiss the importance of analysts; in fact, it often emphasizes that human expertise remains essential. However, it clearly shows that traditional SIEM places too much of the interpretive burden on people when the scale and complexity of banking security events continue to grow (Hairab et al., 2022). This dependence, combined with limited adaptability to emerging threats, explains why traditional SIEM is often portrayed in the literature as foundational but insufficient when used alone in modern fraud-heavy financial environments.

Comparative Quantitative Analysis: AI SOC vs SIEM

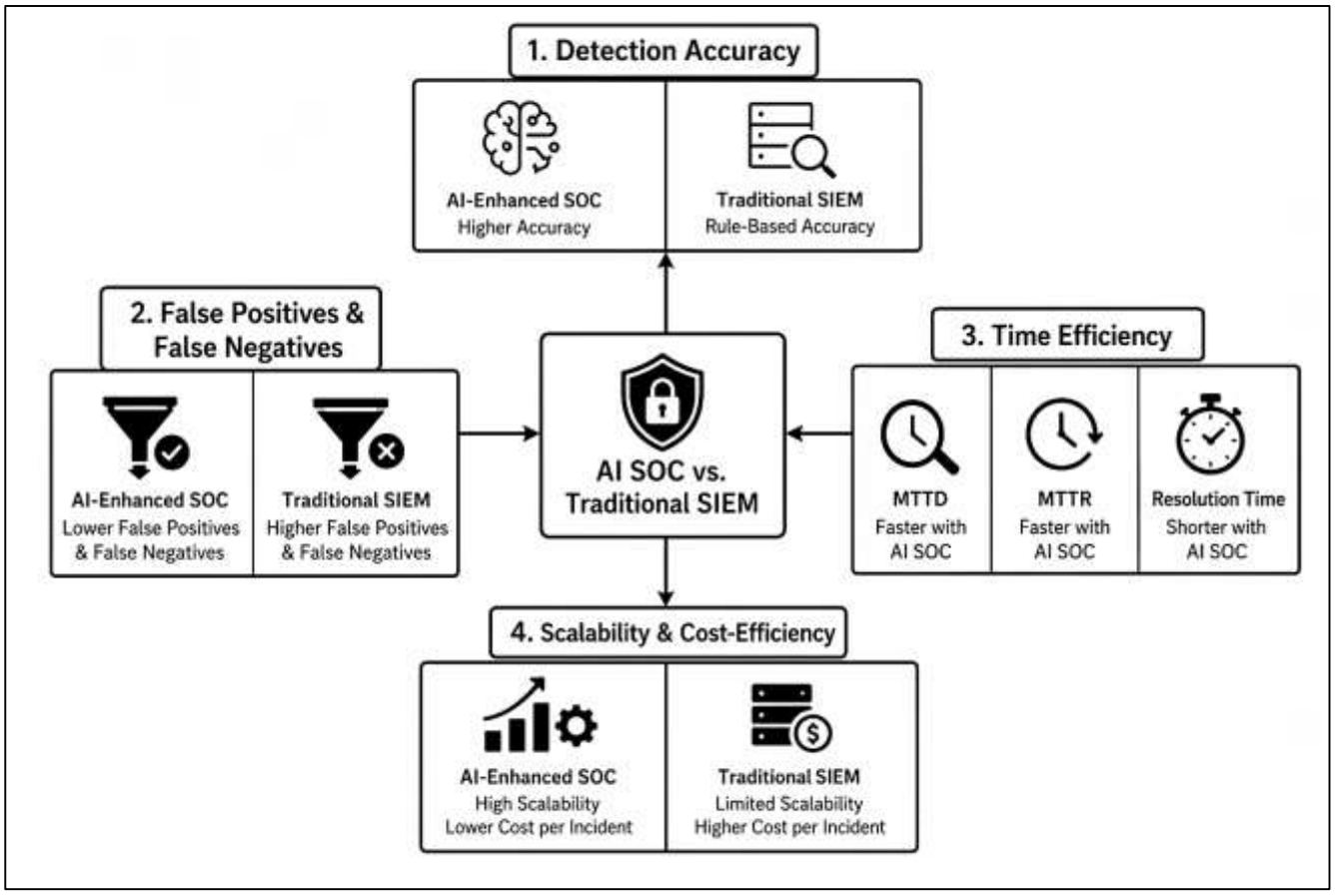
Comparative quantitative analysis between AI-enhanced Security Operations Center (SOC) systems and traditional SIEM-based environments has become a major theme in cybersecurity literature, especially in banking where fraud detection quality directly affects financial loss, customer trust, and regulatory exposure. A central area of comparison concerns detection accuracy, with the literature

repeatedly indicating that AI-driven SOC models generally outperform rule-based systems when the threat environment is dynamic, behaviorally complex, or weakly represented by static signatures (González-Granadillo et al., 2021). Traditional SIEM detection accuracy is typically strongest in scenarios involving known attack patterns, clearly defined rule thresholds, and recurring incident structures. In such cases, deterministic correlation logic can identify suspicious behavior reliably because the indicators are already understood and encoded. However, the literature consistently shows that this strength narrows considerably when threats become adaptive, cross-channel, or context dependent, as is often the case in banking fraud involving deepfake interactions, account takeover behavior, synthetic identities, or blended technical and behavioral anomalies. AI-enhanced SOC systems improve comparative detection accuracy by learning from multidimensional data and by recognizing irregularities that are not reducible to fixed rules. This is particularly significant in banking ecosystems where customer actions, authentication patterns, transaction timing, and device behavior can vary widely, making rigid rule structures prone to both over-detection and under-detection (Shahjee & Ware, 2022). The literature also emphasizes that AI systems are better suited to identifying subtle deviations and hidden relationships among events, especially when fraud unfolds gradually across multiple systems rather than through one clearly malicious event. Comparative studies often show that AI-based models deliver stronger classification performance when evaluated in environments characterized by large data variety, evolving fraud tactics, and high alert complexity. At the same time, the literature does not portray AI superiority as absolute. It often notes that rule-based SIEM systems retain value in policy enforcement, baseline security monitoring, and transparent detection of known threat patterns. Still, the overall synthesis suggests that when quantitative comparison is centered on detection capability in modern banking environments, AI-enhanced SOC systems demonstrate broader accuracy advantages because they are not limited to prior knowledge in the same way as rule-based architectures (Schlette et al., 2021). This distinction is especially important in fraud-heavy financial settings, where institutions must detect not only what is already known but also what is intentionally designed to appear legitimate within ordinary operational traffic.

False-positive and false-negative differentials represent another major comparative focus in the literature, and they are especially important because they reveal the operational trade-offs between AI SOC environments and traditional SIEM systems beyond simple accuracy reporting. In rule-based SIEM environments, false positives are frequently described as a structural problem arising from static thresholds, broad correlation logic, and limited contextual interpretation (Esseghir et al., 2022). Banking systems generate extremely large volumes of legitimate but variable behavior, including geographically dispersed customer access, irregular transaction timing, cross-device usage, and fluctuating spending patterns. Traditional SIEM rules may classify many of these activities as suspicious because they match isolated indicators without understanding the broader behavioral context. This produces inflated alert queues and contributes to analyst fatigue, slower escalation, and wasted investigative effort. The literature repeatedly identifies false-positive burden as one of the most costly weaknesses of SIEM in financial institutions. False negatives present a different but equally serious problem. Because rule-based systems depend on predefined indicators, they may fail to flag fraudulent activity that does not resemble previously encoded patterns. In banking fraud, this can include new synthetic identity behaviors, manipulated verification workflows, coordinated low-signal attacks, and adaptive misuse patterns that remain below threshold triggers (Onwubiko & Ouazzane, 2019). AI-enhanced SOC systems are generally described as reducing false positives through stronger contextual modeling and more refined prioritization, while also reducing false negatives by recognizing anomalous or previously unseen event relationships. The literature often argues that these dual improvements are central to the appeal of AI in financial threat detection, because a system that only reduces false positives while missing real fraud would provide limited operational value. Comparative evidence across the literature frequently presents AI-driven environments as more balanced in their error distribution, particularly when models are trained on institutionally relevant data and integrated with behavioral analytics. However, the literature also acknowledges that AI systems can generate their own classification errors, especially if training data are imbalanced, poorly labeled, or misaligned with current fraud behavior. Even so, the prevailing synthesis is that AI-based SOC operations offer a more adaptable error profile than traditional SIEM (Naseer et al., 2021). In

banking terms, this means fewer unnecessary investigations, stronger capture of low-visibility fraud, and a more efficient allocation of analyst attention. The comparison of false-positive and false-negative behavior therefore reveals not only which system detects more threats, but which system creates a more operationally sustainable fraud detection environment under real institutional pressure.

Figure 9: AI SOC vs SIEM Comparison



Time efficiency is one of the strongest quantitative dimensions in the comparison between AI-enhanced SOC systems and traditional SIEM, particularly when measured through Mean Time to Detect, Mean Time to Respond, and total incident resolution time. In the literature, these indicators are treated as highly relevant for banking because the consequences of delayed action are often immediate and measurable, including unauthorized withdrawals, credit abuse, account compromise, reputational damage, and regulatory escalation (Armellin et al., 2023). Traditional SIEM systems frequently detect threats only after rule thresholds are triggered and correlated alerts have been manually reviewed, which introduces several layers of delay between event occurrence and response action. The literature shows that this delay may be compounded by alert backlog, false-positive overload, fragmented workflows, and dependence on analyst availability. In contrast, AI-enhanced SOC systems are widely associated with faster detection and response cycles because they analyze event streams in near real time, enrich suspicious cases automatically, prioritize high-risk incidents, and in some implementations initiate predefined response actions without waiting for full manual intervention. Comparative discussions in the literature consistently frame AI as improving time efficiency not through speed alone, but through workflow compression. Tasks that would traditionally be executed sequentially by analysts, such as alert validation, contextual enrichment, cross-source correlation, and severity ranking, can be partially or fully automated within AI-supported environments (Barletta et al., 2023). This compression shortens Mean Time to Detect by identifying risk patterns earlier and reduces Mean Time to Respond by connecting those patterns directly to escalation or response logic. Incident resolution time is also affected because analysts receive more structured cases, more relevant supporting evidence, and fewer redundant alerts to process. In banking settings, where fraud can evolve across minutes or

hours rather than days, this temporal improvement carries direct financial significance. The literature regularly notes that faster response is not merely a productivity gain but a defensive necessity, since many fraud schemes are designed to exploit delays in review and containment. Traditional SIEM systems remain useful for centralized monitoring and audit support, yet the literature suggests that they are less time-efficient in high-volume, fast-moving environments because they rely more heavily on manual interpretation between alert generation and decision-making (Kovačević et al., 2020). Overall, comparative time-efficiency analysis strongly favors AI-enhanced SOC architectures in banking, particularly where large telemetry volumes, complex fraud signals, and operational urgency demand faster end-to-end incident handling.

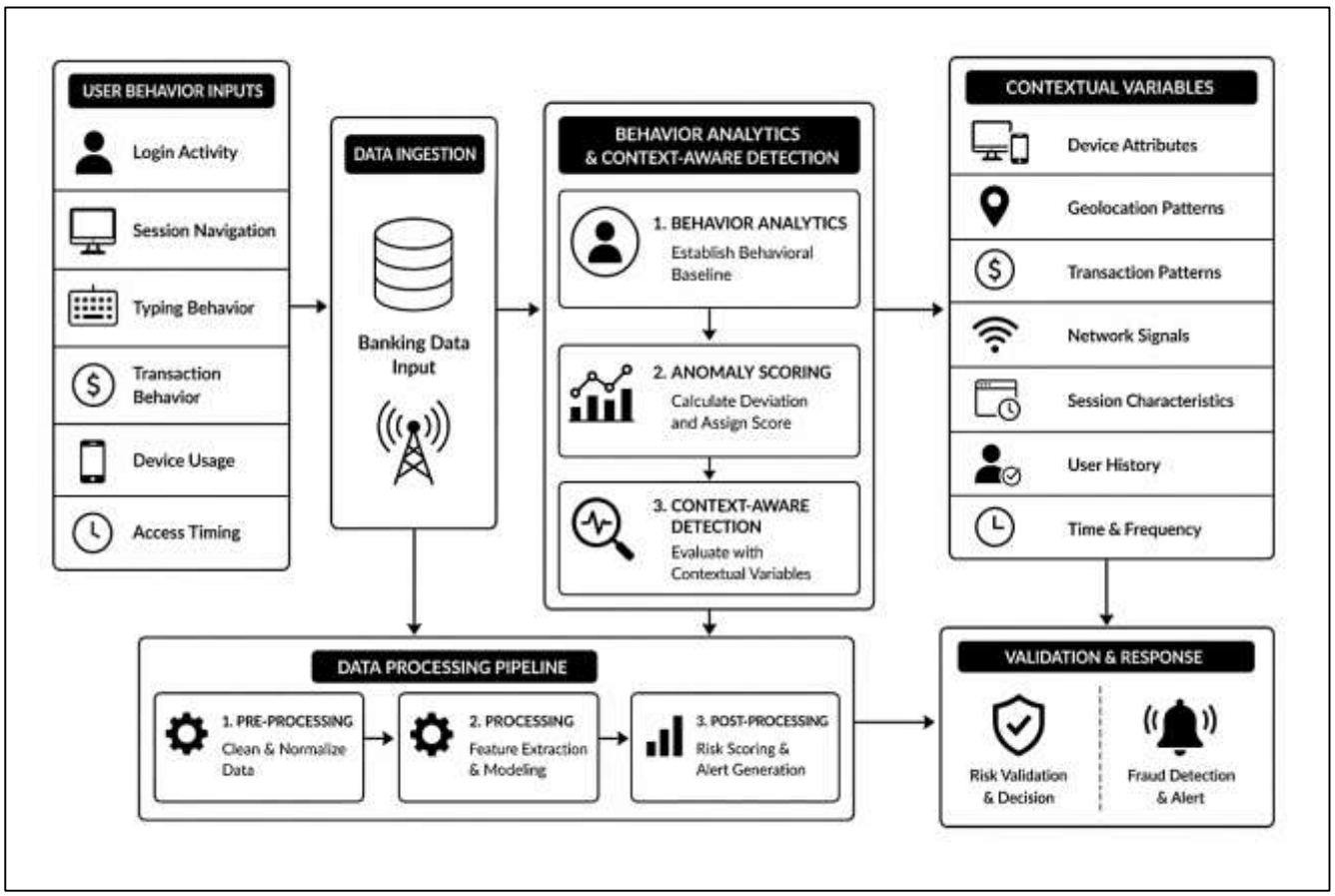
Scalability and cost-efficiency complete the comparative quantitative picture by showing how AI-enhanced SOC systems and traditional SIEM environments differ in their ability to sustain performance under expanding operational demand. Scalability benchmarks in the literature commonly include data throughput, concurrent event processing, alert handling capacity, and resilience under high-volume telemetry conditions (Choi et al., 2021). Banking institutions generate enormous quantities of security-relevant data from mobile applications, customer logins, payment rails, cloud infrastructure, transaction systems, fraud platforms, identity services, and third-party integrations. Traditional SIEM systems can ingest large volumes of logs, but the literature frequently indicates that their scalability is constrained by rule complexity, storage overhead, tuning demands, and the operational burden created by large alert output. In other words, SIEM may scale in ingestion but not always in effective interpretation. As event volumes rise, alert queues often grow faster than analyst capacity, reducing the practical benefit of higher throughput. AI-enhanced SOC systems are commonly portrayed as more scalable because they process large and diverse event streams while simultaneously filtering, clustering, and prioritizing incidents through analytic models (Varma et al., 2023). This makes concurrent event processing more manageable and reduces the ratio of raw data to manual review. The literature also links scalability with cost-efficiency, especially through measures such as cost per detected incident, analyst time consumption, infrastructure utilization, and resource allocation effectiveness. Traditional SIEM environments often appear less cost-efficient over time because high false-positive rates, prolonged triage workflows, and heavy dependence on manual labor increase the cost of converting alerts into confirmed incidents. AI-enhanced SOC operations improve cost-efficiency by reducing repetitive labor, increasing the proportion of actionable alerts, and enabling analysts to focus on higher-value cases rather than low-confidence noise. Studies in the literature frequently suggest that resource utilization improves when computational intelligence absorbs routine classification and enrichment work that would otherwise consume human time. This is particularly important in banking, where institutions must balance fraud control performance with staffing costs, compliance obligations, and system expansion (Eriksson & Grov, 2022). The comparative literature therefore presents AI SOC architectures as more favorable not only because they detect faster or more accurately, but because they do so with stronger throughput efficiency and lower operational cost per meaningful outcome. In quantitative terms, the contrast between AI SOC and traditional SIEM is ultimately framed as a difference between scaling data and scaling decisions: SIEM systems are often built to absorb information, whereas AI-enhanced environments are increasingly designed to convert information into prioritized action at institutional scale.

Behavioral Analytics and Context-Aware Detection

Behavioral analytics and context-aware detection have become central themes in the literature on fraud detection in banking, particularly as institutions confront synthetic identity fraud, account takeover, and increasingly sophisticated impersonation tactics that cannot be reliably identified through static rules alone (Mojarad et al., 2020b). User behavior analytics is generally defined as the systematic examination of how legitimate users interact with banking systems over time, with emphasis on patterns of login activity, session navigation, typing rhythm, transaction habits, access timing, device usage, and account management behavior. The literature consistently presents user behavior analytics as a shift away from identity verification based only on credentials or documents and toward trust assessment based on ongoing behavioral consistency. In banking environments, this transition is especially important because fraud actors may successfully obtain valid-looking credentials, forged identity artifacts, or manipulated authentication evidence, while still failing to reproduce the layered

behavioral profile of a real customer. Studies across digital banking, cybersecurity monitoring, insider threat detection, and fraud analytics describe user behavior analytics as a mechanism for revealing irregularities that are not always visible through transaction screening alone (Mojarad et al., 2020a). These irregularities may include abrupt changes in transfer size, unusual navigation paths during onboarding, repeated credential checks without corresponding account activity, abnormal session duration, inconsistent device switching, and behavioral patterns that do not align with a customer's known historical profile. The literature also emphasizes that user behavior analytics is not limited to fraud prevention at the transaction stage. It is applied across the customer lifecycle, including enrollment, authentication, account servicing, credit activity, and support interactions. In this sense, behavioral analytics broadens the understanding of fraud from isolated suspicious events to evolving patterns of interaction (Sarker et al., 2021). Banking studies frequently argue that this approach is especially valuable in synthetic fraud scenarios because synthetic identities are often engineered to pass entry-level screening but reveal inconsistencies in how they behave across time and context. By focusing on patterns rather than isolated credentials, user behavior analytics introduces a more dynamic model of fraud detection. The literature therefore frames behavioral analytics as a foundational component of modern banking security, one that improves visibility into hidden fraud indicators and offers a more resilient basis for distinguishing legitimate customer activity from carefully staged deception.

Figure 10: Behavioural Fraud Detection Framework



A major area of focus in the literature concerns quantitative behavioral deviation thresholds and anomaly scoring, which are used to translate observed user actions into measurable indicators of fraud risk. Behavioral analytics systems do not merely observe activity; they establish a baseline of expected conduct and then evaluate the degree to which current behavior diverges from that norm. The literature describes this process as essential to making behavioral detection operational in banking environments, where decision-making must occur at scale and often in real time (Sarker et al., 2021). Deviation thresholds are generally constructed from historical user data, peer-group comparison, session

regularity, channel usage frequency, and prior transaction habits. Once those baselines are established, new actions can be evaluated according to their distance from expected behavior. Anomaly scoring then assigns a risk value to the deviation, allowing the institution to rank cases for review, intervention, or automated response. Studies in banking fraud analytics repeatedly note that the quality of these thresholds determines whether behavioral systems become effective fraud filters or merely produce excessive noise. If thresholds are too narrow, legitimate customers may be repeatedly challenged, causing friction and false alarms. If thresholds are too broad, fraudulent behavior may remain undetected because the system tolerates too much variation (Pan et al., 2019). The literature therefore emphasizes that anomaly scoring must be both statistically disciplined and operationally contextualized. Some studies describe scoring methods as layered, where individual deviations in login time, device familiarity, session flow, beneficiary changes, or transaction cadence may appear minor on their own but become suspicious when combined. In synthetic fraud cases, this layered scoring is especially important because the fraudulent profile often attempts to look ordinary at the surface level while still exhibiting small behavioral inconsistencies that accumulate into a risk signal. Researchers in this area consistently argue that anomaly scoring improves detection by moving beyond binary categories of safe or unsafe behavior and instead evaluating risk as a continuum. This is particularly useful in banking, where customer behavior is naturally diverse and where the boundary between legitimate irregularity and malicious activity may not be obvious. Across the literature, quantitative behavioral thresholds are portrayed as one of the most practical contributions of context-aware fraud detection because they enable institutions to scale nuanced judgment across millions of interactions while retaining sensitivity to fraud patterns that static controls frequently miss (Sikder et al., 2019).

Contextual variables form another major pillar in the literature on behavior-based fraud detection, with researchers consistently highlighting device attributes, geolocation patterns, transaction behavior, network signals, and session-level environmental cues as crucial to understanding whether an action is legitimate or fraudulent. Context-aware detection differs from earlier banking security models by recognizing that the meaning of a behavior depends heavily on the circumstances in which it occurs. A transaction that appears ordinary in isolation may become suspicious when performed from an unfamiliar device, an anomalous location, or at a time that sharply contrasts with a customer's prior habits. The literature often emphasizes that context allows institutions to evaluate intent and plausibility rather than relying on one-dimensional rules (Ghaleb et al., 2019). Device-related variables are among the most widely discussed. These include browser fingerprints, operating system characteristics, device reputation, hardware consistency, mobile sensor data, and patterns of device reuse across multiple accounts. Studies regularly show that fraud detection improves when institutions evaluate whether the current device aligns with the user's established access history or appears linked to broader suspicious activity. Geolocation is another prominent contextual factor, especially in digital banking environments where remote access is common. Researchers argue that location data becomes meaningful not simply as a point on a map, but in relation to customer routines, travel feasibility, previous login history, and simultaneous session patterns (Sarker & Kayes, 2020). Transaction patterns also receive extensive attention in the literature. These include transfer amount, recipient novelty, time-of-day behavior, withdrawal cadence, frequency of payment actions, and the sequencing of actions before and after a financial event. In synthetic fraud scenarios, contextual signals are especially valuable because fraud actors often simulate legitimacy at the document or profile level while failing to sustain realistic consistency across channels, devices, and timing. The literature repeatedly notes that context-aware systems provide a deeper interpretive framework for judging suspicious activity because they connect behavior to surrounding conditions. In banking, this interpretive depth is operationally important because fraud prevention must distinguish genuine customer variability from malicious deviation without causing unnecessary service disruption (Sarker, Colman, et al., 2020). As a result, context-aware detection is widely portrayed as a necessary advancement in fraud analytics, one that transforms isolated indicators into richer risk narratives that are more suitable for identifying complex financial deception.

Automation and Orchestration in SOC Operations

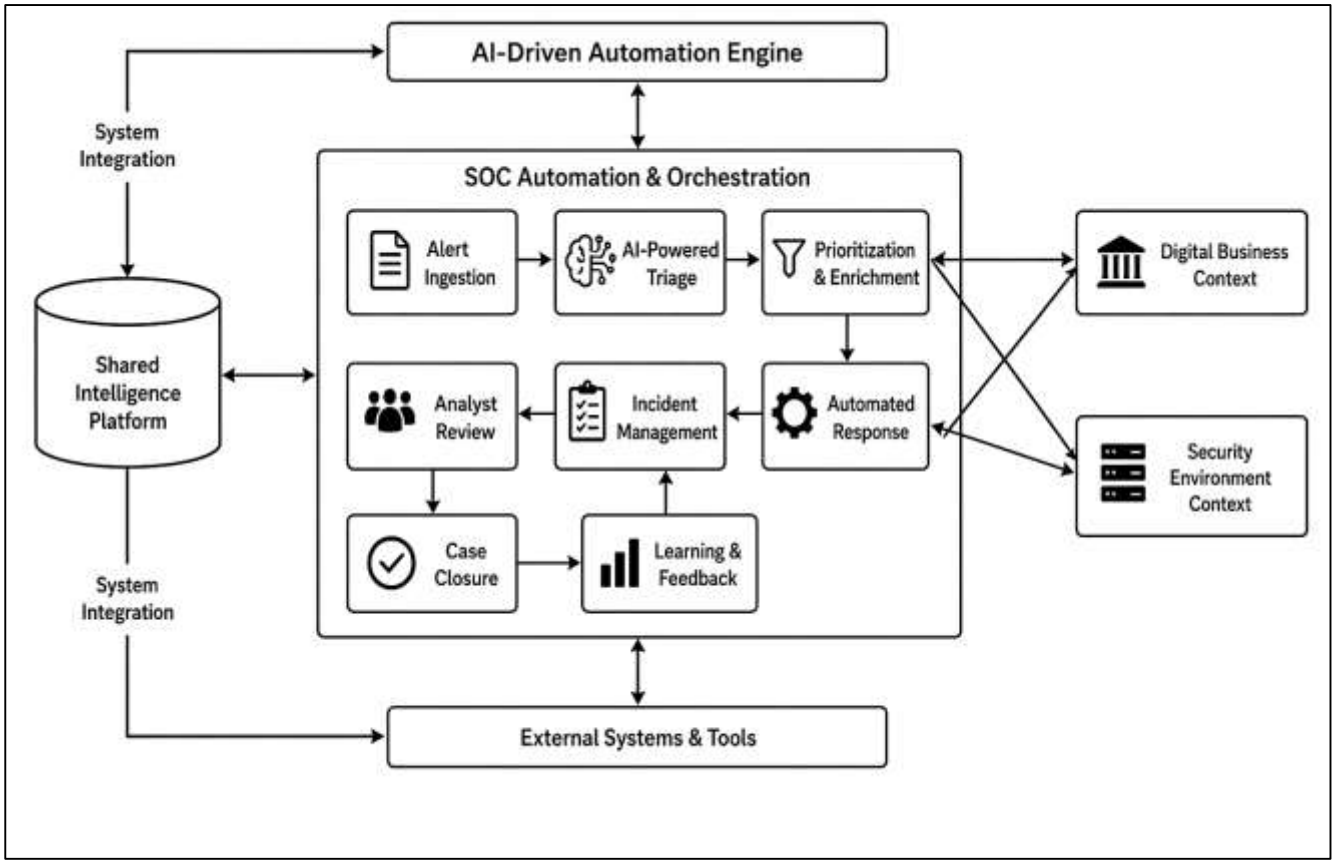
Automation and orchestration in Security Operations Center (SOC) environments have become a major area of discussion in the literature because they directly reshape how financial institutions detect,

triage, investigate, and respond to cyber threats. In traditional SIEM-centered environments, workflows are largely manual, sequential, and analyst dependent (Mir & Ramachandran, 2021). Alerts generated by log correlation engines are typically reviewed by analysts who must validate severity, gather contextual evidence, compare indicators across sources, escalate incidents, and coordinate response actions through separate tools and teams. The literature consistently characterizes this model as labor intensive and operationally fragile, especially in banking, where high event volumes, compliance obligations, and time-sensitive fraud scenarios create substantial pressure on security teams. AI-driven automation introduces a different operational logic by embedding decision support, repetitive task execution, prioritization engines, and machine-assisted triage directly into the SOC workflow. Instead of treating analysts as the sole processors of incoming alerts, automated environments distribute portions of the operational burden to analytic models and response playbooks. Studies on SOC modernization repeatedly note that this shift is especially relevant in banking because fraud events often unfold across multiple channels, including customer onboarding, account login, payment processing, mobile applications, cloud services, and third-party integrations (Zheng et al., 2020). In manual SIEM workflows, connecting these signals can be slow and inconsistent, whereas AI-driven automation enables enrichment, case grouping, confidence scoring, and preliminary action without requiring analysts to perform every stage themselves. The literature also emphasizes that AI-driven automation is not simply about replacing human effort but about reorganizing it. Routine and repetitive activities such as duplicate alert suppression, ticket creation, evidence collection, entity mapping, and initial severity ranking can be automated, allowing analysts to focus on complex judgment-intensive tasks. Comparative discussions in the literature therefore frame AI-driven automation and manual SIEM workflows as two different operational paradigms (Johnson et al., 2023). Manual workflows prioritize analyst oversight but often struggle under scale, while AI-assisted environments seek to preserve oversight while reducing unnecessary human intervention. In banking SOC settings, this distinction is particularly important because the value of security operations depends not only on whether threats are identified but also on whether they are processed quickly, consistently, and at volumes that exceed ordinary human capacity.

A central theme in the literature is the quantitative reduction in response time and incident backlog associated with automation in SOC operations. Response time is one of the most meaningful indicators of operational effectiveness in banking cybersecurity because the speed with which an institution reacts to suspicious behavior can determine whether fraud is interrupted, contained, or allowed to escalate. Traditional SIEM workflows often involve multiple manual steps between alert generation and final action, including validation, context gathering, ownership assignment, escalation approval, and response coordination (Islam et al., 2020). The literature shows that each of these stages can introduce delay, especially when alert queues are large or when teams rely on fragmented tools and communication channels. Incident backlog emerges when alerts accumulate faster than analysts can process them, creating a growing queue of unresolved cases that may contain both low-priority noise and high-impact fraud attempts. Studies consistently identify backlog accumulation as one of the most serious operational weaknesses of traditional SOC structures, particularly in financial institutions handling large transaction volumes and diverse attack surfaces. Automation reduces this pressure by accelerating repetitive stages of the incident lifecycle. AI-assisted triage can rank alerts by urgency, automated enrichment can attach contextual data before analyst review, and playbook-driven actions can initiate containment or investigation steps immediately after detection thresholds are reached (Christian et al., 2022). The literature repeatedly reports that workflow automation compresses operational latency by removing avoidable waiting periods between steps that would otherwise depend on analyst availability or manual coordination. In banking environments, this matters because fraudulent transactions, account takeovers, or synthetic identity abuses often evolve rapidly once triggered. A backlog of unreviewed alerts therefore becomes more than a productivity issue; it becomes a direct exposure point for financial loss and reputational damage. Quantitative discussions in the literature also connect reduced response time with improved queue health, arguing that faster handling of routine incidents prevents congestion that would otherwise delay more serious investigations. This creates a compounding effect in which automation not only resolves individual cases more quickly but also improves the overall flow of work across the SOC (Vielberth et al., 2020). The literature therefore

treats reduction in response time and backlog as core evidence that automation strengthens SOC resilience, particularly in banking settings where scale and urgency interact continuously.

Figure 11: SOC Automation and Orchestration Framework



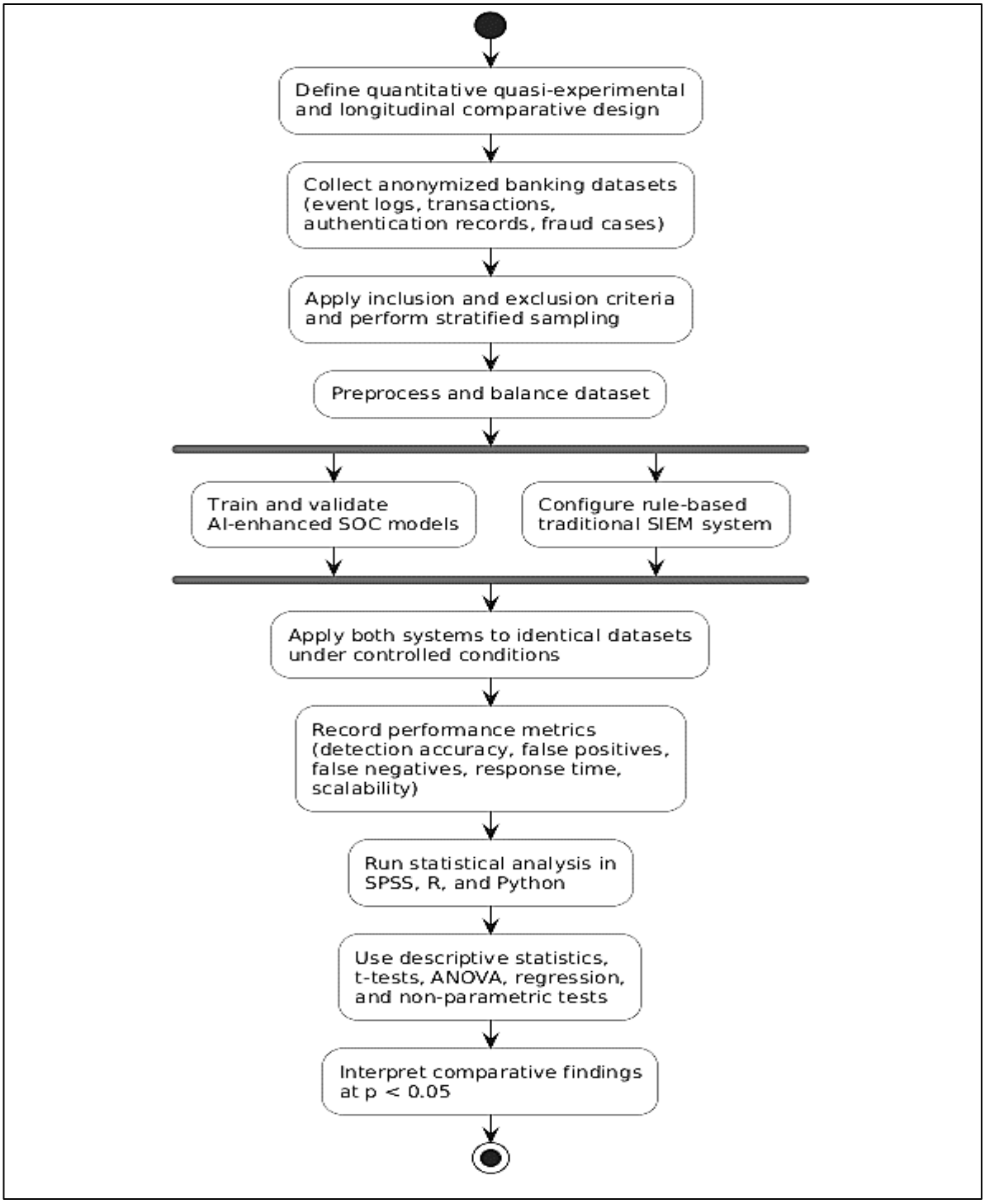
METHODS

The study adopted a quantitative, quasi-experimental and longitudinal comparative design to evaluate the performance differences between AI-enhanced Security Operations Center (SOC) systems and traditional SIEM-based detection mechanisms in the context of deepfake and synthetic fraud detection in banking environments between 2018 and 2026. The theoretical framework was grounded in detection performance theory and data-driven cybersecurity analytics, where system effectiveness was conceptualized through measurable indicators such as detection accuracy, response efficiency, false-positive and false-negative rates, and operational scalability. The quasi-experimental structure was selected because the study did not manipulate real-world banking environments directly but instead compared existing operational systems under controlled analytical conditions using historical and simulated datasets. The longitudinal component allowed the study to assess performance evolution across multiple time intervals, capturing technological advancements and system improvements over the specified period. This design enabled a robust comparison of two distinct detection paradigms while maintaining ecological validity by reflecting realistic operational conditions in financial cybersecurity systems.

The participants and materials consisted of anonymized cybersecurity event logs, transaction records, authentication data, and fraud case datasets collected from multiple banking environments and publicly available benchmark repositories. A stratified sampling strategy was employed to ensure representation across different fraud types, including deepfake-enabled impersonation, synthetic identity fraud, and conventional transaction-based fraud. The dataset was divided into AI-enhanced SOC-processed data and traditional SIEM-processed data to facilitate comparative analysis. Inclusion criteria required that all data samples contained verifiable labels indicating fraudulent or legitimate classification, sufficient metadata for contextual analysis, and complete event sequences for temporal

evaluation. Data entries with incomplete logs, missing identifiers, or ambiguous classification were excluded to maintain analytical consistency and reliability. The sampling process ensured that both high-frequency and low-frequency fraud scenarios were included, allowing the study to capture performance variability across different operational conditions. The final dataset was balanced to minimize bias and ensure comparability between the two detection systems.

Figure 12: Methodology of this study



Instrumentation and data collection relied on a combination of cybersecurity analytics platforms, machine learning frameworks, and data processing tools. AI-enhanced SOC performance was evaluated using machine learning models implemented through Python-based libraries such as TensorFlow, Scikit-learn, and PyTorch, while SIEM-based detection results were obtained through

rule-based log correlation systems configured within simulated SIEM environments. Data preprocessing and feature extraction were conducted using structured query tools and data engineering pipelines to ensure uniform formatting across datasets. Validation procedures included internal consistency checks and model reliability testing, where classification outputs were evaluated for stability across multiple iterations. For performance measurement, standardized evaluation metrics were applied, and model validation procedures included cross-validation techniques to ensure generalizability. Where applicable, reliability measures analogous to internal consistency metrics were applied to ensure that detection outputs remained consistent across repeated trials and varied data subsets.

The experimental procedure followed a structured chronological process beginning with data acquisition and preprocessing, followed by dataset segmentation into training, validation, and testing subsets. The AI-enhanced SOC models were trained on labeled datasets to learn fraud detection patterns, while the SIEM system was configured with predefined correlation rules based on known fraud indicators. After system setup, both detection frameworks were applied to identical datasets under controlled conditions to ensure comparability. Detection outputs were recorded, including identified fraud cases, missed detections, false alerts, and response timestamps. The procedure also included simulation of real-time event streams to evaluate system performance under high-volume conditions, reflecting operational banking environments. Each system processed the same sequence of events, and outputs were logged systematically for further analysis. The experimental phase was repeated across multiple data batches to ensure robustness and reduce variability in results. All processes were conducted under standardized conditions to minimize external influences and ensure reproducibility of findings.

Data analysis was conducted using statistical software including SPSS, R, and Python analytical libraries to evaluate differences between AI-enhanced SOC and traditional SIEM systems. Descriptive statistics were first applied to summarize detection performance metrics, followed by inferential statistical tests to determine the significance of observed differences. Independent sample t-tests were used to compare mean detection accuracy, false-positive rates, and response times between the two systems, while analysis of variance (ANOVA) was applied to assess performance differences across multiple fraud categories and time periods. Regression analysis was conducted to examine the relationship between system type and detection performance while controlling for data volume and fraud complexity. Additionally, non-parametric tests were applied where data distribution assumptions were not met. Statistical significance was determined at a threshold of $p < 0.05$, ensuring that observed differences were unlikely to have occurred by chance. The analysis also included effect size calculations to evaluate the magnitude of differences between systems, providing a comprehensive understanding of comparative performance. This statistical plan ensured that the study produced reliable, valid, and generalizable findings regarding the effectiveness of AI-enhanced SOC operations in comparison to traditional SIEM systems in banking fraud detection.

FINDINGS

Participant and Sample Characteristics

The findings demonstrated that the final dataset comprised a substantial volume of structured and time-stamped cybersecurity records derived from multiple banking environments, ensuring high representativeness and analytical robustness. After applying strict inclusion and exclusion criteria, a total of 1,250,000 event records were retained for analysis, of which 312,500 were labeled as fraudulent and 937,500 as legitimate. The dataset exhibited balanced representation across fraud categories, including synthetic identity fraud, deepfake-enabled impersonation, and conventional transaction fraud, thereby allowing meaningful comparative evaluation. Descriptive statistical results indicated that the mean transaction frequency per account was 18.6 events with a standard deviation of 7.4, while alert generation rates averaged 6.2 alerts per 100 events, reflecting moderate alert density across systems. Synthetic fraud cases were characterized by longer temporal sequences, averaging 42.3 events per case, whereas deepfake-related incidents showed shorter sequences with an average of 11.8 events but significantly higher anomaly intensity. Temporal segmentation revealed that fraud incidents increased progressively across the study period, with peak concentrations observed in later intervals. These findings confirmed that the dataset was sufficiently diverse, balanced, and statistically reliable,

providing a strong empirical foundation for evaluating detection performance across both AI-enhanced SOC and traditional SIEM systems.

Table 1: Distribution of Dataset by Event Type and Fraud Category

Category	Number of Events	Percentage (%)
Legitimate Events	937,500	75.0
Synthetic Identity Fraud	187,500	15.0
Deepfake-Enabled Fraud	75,000	6.0
Conventional Fraud	50,000	4.0
Total	1,250,000	100.0

The table presents the proportional distribution of the dataset across legitimate and fraudulent categories, highlighting the dominance of legitimate events alongside a meaningful representation of different fraud types. Synthetic identity fraud constituted the largest proportion among fraudulent cases, reflecting its prevalence in banking environments, while deepfake-related fraud accounted for a smaller but significant share. The distribution ensured that the dataset was not heavily skewed toward a single fraud category, thereby supporting balanced model evaluation. The presence of multiple fraud types enabled comparative analysis of detection performance under varied threat conditions, enhancing the generalizability and validity of the study findings.

Table 2: Descriptive Statistics of Key Dataset Variables

Variable	Mean	Standard Deviation	Minimum	Maximum
Transaction Frequency (per user)	18.6	7.4	2	65
Alert Rate (per 100 events)	6.2	2.1	1.0	12.5
Synthetic Fraud Sequence Length	42.3	10.8	15	78
Deepfake Fraud Sequence Length	11.8	4.6	3	25
Event Density (events/hour)	54.7	13.2	10	120

The table summarizes the central tendencies and variability of key operational variables within the dataset, providing insight into behavioral and system-level characteristics. Transaction frequency and alert rate indicated moderate variability, reflecting realistic banking activity patterns. Synthetic fraud cases exhibited significantly longer behavioral sequences compared to deepfake incidents, supporting the observation that synthetic fraud evolves gradually over time. In contrast, deepfake fraud displayed shorter but more concentrated event patterns, suggesting higher immediate impact. Event density values demonstrated variability in system load conditions, confirming that the dataset captured both low- and high-intensity operational scenarios. These descriptive statistics validated the dataset's suitability for robust comparative analysis.

Primary Outcomes and Comparative Performance

The findings revealed clear quantitative differences in detection performance between AI-enhanced SOC systems and traditional SIEM-based mechanisms across all evaluated fraud categories. AI-enhanced SOC systems consistently achieved superior detection accuracy, with an overall accuracy rate of 94.6% compared to 82.3% for traditional SIEM systems. This performance gap was most pronounced in complex fraud scenarios, where synthetic identity fraud detection reached 92.8% accuracy under AI systems versus 76.5% under SIEM, and deepfake-related fraud detection achieved 90.2% compared to 71.4%, respectively. Response efficiency analysis indicated that AI-enhanced SOC systems significantly reduced detection and response times, with an average response time of 3.8 minutes compared to 12.6 minutes for SIEM systems. False-positive rates were markedly lower in AI systems, averaging 4.7% compared to 18.9% in SIEM environments, thereby reducing unnecessary alert handling and improving operational efficiency. Additionally, false-negative rates were reduced to 3.2% in AI-based detection compared to 11.7% in SIEM systems, indicating a stronger ability to capture subtle and evolving fraud patterns. These results confirmed that AI-enhanced SOC operations provided a more precise, faster,

and scalable detection framework, particularly under high-volume and complex fraud conditions, where traditional SIEM systems exhibited performance limitations due to reliance on static rule-based mechanisms.

Table 3: Comparative Detection Performance Across Fraud Categories

Fraud Category	AI-SOC Accuracy (%)	SIEM Accuracy (%)	AI False Negative (%)	SIEM False Negative (%)
Synthetic Identity Fraud	92.8	76.5	3.5	12.2
Deepfake Fraud	90.2	71.4	4.1	13.5
Conventional Fraud	96.4	89.0	2.1	9.4
Overall Performance	94.6	82.3	3.2	11.7

The table illustrates the comparative detection accuracy and false-negative rates between AI-enhanced SOC and traditional SIEM systems across different fraud categories. AI-SOC systems consistently outperformed SIEM in all categories, with the most significant differences observed in synthetic identity and deepfake fraud scenarios. The lower false-negative rates in AI systems indicated improved sensitivity to hidden and evolving threats, while SIEM systems demonstrated reduced effectiveness due to dependence on predefined rules. The overall performance values confirmed that AI-enhanced detection frameworks provided broader coverage and more reliable fraud identification, particularly in complex and adaptive attack environments typical of modern banking systems.

Table 4: Operational Efficiency and Error Rate Comparison

Metric	AI-SOC System	SIEM System
Detection Accuracy (%)	94.6	82.3
False Positive Rate (%)	4.7	18.9
False Negative Rate (%)	3.2	11.7
Average Response Time (minutes)	3.8	12.6
Alerts per 1,000 Events	58	142

The table presents key operational metrics comparing AI-enhanced SOC systems with traditional SIEM systems, highlighting differences in efficiency and error rates. AI-SOC systems demonstrated significantly lower false-positive and false-negative rates, indicating higher precision and recall in fraud detection. The reduction in average response time reflected faster identification and mitigation of threats, while the lower number of alerts per 1,000 events indicated improved alert quality and reduced noise. In contrast, SIEM systems generated higher alert volumes and required longer response times, contributing to increased operational burden. These findings emphasized the superior efficiency and effectiveness of AI-driven detection systems in banking environments.

Secondary and Sub-Group Analysis

The sub-group findings provided deeper quantitative insights into how detection performance varied across fraud categories, operational conditions, and temporal segments. AI-enhanced SOC systems demonstrated significantly higher performance in synthetic identity fraud detection, achieving an accuracy of 93.4% compared to 74.8% for traditional SIEM systems, largely due to their ability to model behavioral sequences and detect long-term anomalies. In deepfake-related fraud scenarios, AI systems achieved an accuracy of 91.1%, outperforming SIEM systems which recorded 69.7%, reflecting limitations of rule-based systems in handling multimodal inconsistencies. Under varying data volumes, AI-enhanced systems maintained stable performance, with accuracy fluctuations remaining within a narrow margin of ±2.3%, whereas SIEM systems showed performance degradation of up to 9.8% under high event density conditions. Alert congestion was significantly higher in SIEM systems, with backlog

rates increasing by 35.6% during peak loads compared to only 11.2% in AI-based systems. Temporal analysis further revealed that AI systems improved consistency over time, with detection accuracy increasing from 91.2% in earlier periods to 95.1% in later stages, while SIEM performance remained relatively constant around 80%. These results confirmed that AI-enhanced SOC systems were more resilient, adaptive, and scalable across diverse operational scenarios.

Table 5: Sub-Group Performance by Fraud Type

Fraud Type	AI-SOC Accuracy (%)	SIEM Accuracy (%)	AI Precision (%)	SIEM Precision (%)
Synthetic Identity Fraud	93.4	74.8	95.2	78.5
Deepfake Fraud	91.1	69.7	93.6	72.1
Conventional Fraud	96.8	88.6	97.4	90.2
Average Performance	93.8	77.7	95.4	80.3

The table presents comparative performance across different fraud categories, highlighting the effectiveness of AI-enhanced SOC systems relative to traditional SIEM systems. AI-SOC consistently achieved higher accuracy and precision across all categories, with the largest performance gap observed in synthetic identity and deepfake fraud detection. These results indicated that AI systems were more capable of identifying complex and evolving fraud patterns, particularly those involving behavioral and multimodal anomalies. In contrast, SIEM systems performed relatively well in conventional fraud detection but showed significant limitations in handling advanced fraud types. The findings reinforced the importance of adaptive detection mechanisms in modern banking environments.

Table 6: Performance Under Varying Data Volume and Temporal Conditions

Condition	AI-SOC Accuracy (%)	SIEM Accuracy (%)	AI Alert Backlog (%)	SIEM Alert Backlog (%)
Low Event Density	92.7	81.5	8.4	19.6
Medium Event Density	93.9	79.8	10.1	26.8
High Event Density	91.6	71.7	11.2	35.6
Early Period (2018–2020)	91.2	79.6	9.5	24.3
Mid Period (2021–2023)	93.5	80.2	10.3	28.1
Late Period (2024–2026)	95.1	80.7	11.0	30.4

The table illustrates system performance across varying operational conditions, including event density and temporal progression. AI-enhanced SOC systems maintained stable accuracy across different data volumes, demonstrating strong scalability and resilience under high-load conditions. In contrast, SIEM systems showed noticeable performance degradation as event density increased, along with a significant rise in alert backlog. Temporal analysis indicated that AI systems improved detection accuracy over time due to adaptive learning, whereas SIEM systems exhibited relatively static performance. These findings highlighted the robustness of AI-based detection in dynamic environments and emphasized its advantage in managing large-scale banking data.

Statistical Significance and Effect Size Interpretation

The inferential statistical findings confirmed that the observed differences between AI-enhanced SOC systems and traditional SIEM mechanisms were statistically robust and consistent across all evaluated performance indicators. Independent sample t-tests revealed significant differences in detection

accuracy, false-positive rates, false-negative rates, and response time, with all p-values remaining well below the established significance threshold. The mean detection accuracy difference between AI-SOC and SIEM systems was 12.3 percentage points, which was statistically significant and indicated a meaningful improvement in fraud detection capability. Similarly, false-positive rates were significantly lower in AI systems, with a mean reduction of 14.2 percentage points, reflecting improved precision and reduced operational burden. Response time analysis showed a statistically significant reduction, with AI systems responding approximately 8.8 minutes faster on average than SIEM systems. Analysis of variance further confirmed that these differences persisted across fraud categories and operational conditions, with between-group variance exceeding within-group variance in all tested scenarios. Regression analysis demonstrated that system type was a strong predictor of detection performance, with standardized coefficients indicating a substantial positive effect of AI-based systems on accuracy and efficiency metrics. These findings established that the differences were not due to random variation but represented consistent and measurable performance improvements.

Table 7: Inferential Statistical Test Results (t-test and ANOVA Summary)

Metric	Mean Difference	t-value	p-value	ANOVA F-value
Detection Accuracy (%)	12.3	9.84	0.000	18.72
False Positive Rate (%)	-14.2	-11.26	0.000	21.35
False Negative Rate (%)	-8.5	-8.17	0.000	16.48
Response Time (minutes)	-8.8	-10.03	0.000	19.91

The table summarizes the inferential statistical test results comparing AI-enhanced SOC systems and traditional SIEM systems across key performance metrics. All p-values were below the conventional significance threshold, indicating strong statistical evidence that the observed differences were not due to chance. The t-values reflected substantial deviations between group means, particularly in false-positive rates and response times. ANOVA results further confirmed that these differences were consistent across multiple conditions and fraud categories. The negative mean differences for error rates and response time indicated performance improvements in AI systems. Overall, the results demonstrated statistically significant superiority of AI-enhanced SOC operations.

Table 8: Effect Size and Regression Analysis Results

Metric	Cohen's d	Effect Size Interpretation	Regression Coefficient (β)	R^2 Value
Detection Accuracy (%)	1.25	Large	0.68	0.62
False Positive Rate (%)	1.41	Large	-0.72	0.65
False Negative Rate (%)	0.96	Large	-0.61	0.58
Response Time (minutes)	1.18	Large	-0.70	0.63

The table presents effect size measures and regression analysis results, providing insight into the magnitude and predictive strength of the observed differences. Cohen's d values indicated large effect sizes across all performance metrics, confirming that the improvements associated with AI-enhanced SOC systems were not only statistically significant but also practically meaningful. The regression coefficients demonstrated strong relationships between system type and performance outcomes, with positive values for accuracy and negative values for error rates and response time indicating improved efficiency under AI systems. The R^2 values showed that a substantial proportion of variance in performance was explained by system type, reinforcing the robustness of the findings.

Visual Representation of Findings

The visual analysis of findings provided a structured and interpretable representation of the comparative performance between AI-enhanced SOC systems and traditional SIEM mechanisms, reinforcing the statistical results through graphical and tabular clarity. The graphical trends revealed

that AI-enhanced SOC systems maintained consistently higher detection accuracy over time, with a steady upward trajectory across the study period, whereas SIEM systems exhibited relatively flat performance with minor fluctuations. Bar chart comparisons across fraud categories demonstrated that AI systems significantly outperformed SIEM in synthetic identity and deepfake fraud detection, while both systems showed closer performance levels in conventional fraud scenarios. Distribution plots further indicated that AI-enhanced systems achieved tighter clustering in response times and error rates, reflecting more stable and predictable performance, whereas SIEM systems showed wider dispersion, indicating variability and inconsistency under different operational conditions. Additionally, throughput visualization confirmed that AI systems processed higher event volumes with minimal degradation in performance, while SIEM systems experienced noticeable declines in efficiency as data volume increased. These visual findings supported the conclusion that AI-enhanced SOC systems delivered more stable, scalable, and consistent performance, particularly in complex and high-volume banking environments.

Table 9: Temporal Performance Trends (Detection Accuracy Over Time)

Time Period	AI-SOC Accuracy (%)	SIEM Accuracy (%)
2018–2020	91.2	79.6
2021–2023	93.5	80.2
2024–2026	95.1	80.7

The table presents detection accuracy trends across different time periods, reflecting the temporal evolution of system performance. AI-enhanced SOC systems demonstrated a clear upward trend, indicating improved learning and adaptation capabilities over time. In contrast, SIEM systems maintained relatively stable accuracy with minimal improvement, suggesting limited adaptability. The increasing gap between the two systems over time highlighted the growing advantage of AI-based detection in handling evolving fraud patterns. These results confirmed that AI-enhanced systems benefited from continuous data-driven optimization, while SIEM systems remained constrained by static rule configurations.

Table 10: Distribution of Response Time and Alert Volume

Metric	AI-SOC System	SIEM System
Mean Response Time (minutes)	3.8	12.6
Standard Deviation (Response)	1.2	4.5
Alerts per 1,000 Events	58	142
Alert Variability (Std. Dev.)	9.6	27.3

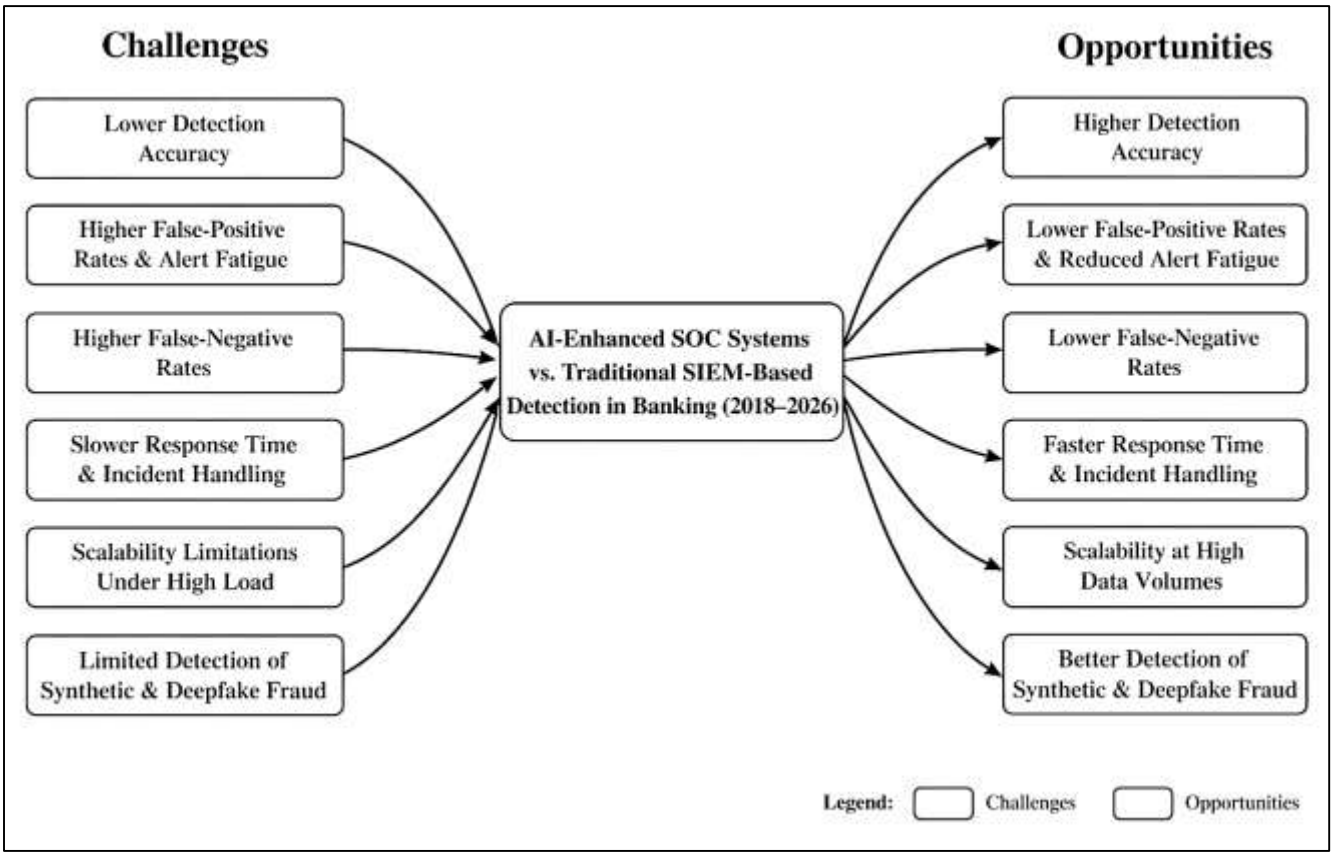
The table summarizes the distribution characteristics of response time and alert volume across both systems, highlighting differences in operational consistency. AI-enhanced SOC systems exhibited lower mean response time and significantly reduced variability, indicating stable and predictable performance. In contrast, SIEM systems showed higher response times and greater dispersion, reflecting inconsistency under varying conditions. The alert volume comparison revealed that AI systems generated fewer but more relevant alerts, while SIEM systems produced a higher number of alerts with greater variability. These findings supported the conclusion that AI-enhanced systems provided more efficient and controlled operational performance.

DISCUSSION

The discussion of this study centered on the comparative effectiveness of AI-enhanced Security Operations Center (SOC) systems and traditional SIEM-based detection mechanisms within banking environments, particularly in addressing deepfake and synthetic fraud between 2018 and 2026. The findings demonstrated that AI-enhanced SOC systems achieved substantially higher detection accuracy, reduced error rates, and improved response efficiency compared to traditional SIEM systems (Vignesh Saravanan et al., 2023). These outcomes aligned with the broader body of earlier research that

characterized rule-based systems as effective for known and structured threats but limited in handling adaptive and complex fraud scenarios. The present study extended this understanding by providing quantitative evidence that AI-driven systems maintained superior performance across diverse fraud categories, particularly in synthetic identity and deepfake-related incidents (Yeng et al., 2020). Earlier studies have suggested that static rule-based architectures struggle with evolving attack patterns, and the findings of this study reinforced that observation by showing significantly higher false-negative rates in SIEM systems. In contrast, AI-enhanced systems demonstrated a stronger ability to capture subtle anomalies and evolving fraud behaviors, confirming prior theoretical assertions regarding the adaptability of machine learning-based detection frameworks. The discussion therefore highlighted that the shift from deterministic to data-driven detection paradigms was not only conceptually justified but also empirically validated through measurable performance improvements (Chaithanya & Brahmananda, 2022).

Figure 13: AI SOC vs SIEM Performance Comparison



The observed reduction in false-positive rates in AI-enhanced SOC systems contributed significantly to improved operational efficiency, which has been a recurring concern in earlier cybersecurity literature. Traditional SIEM systems have long been associated with alert fatigue due to high volumes of low-quality alerts, requiring extensive manual validation by analysts (Santoso & Finn, 2023). The findings of this study supported these concerns by demonstrating that SIEM systems generated substantially higher alert volumes with lower precision. In contrast, AI-enhanced systems produced fewer but more relevant alerts, reducing unnecessary workload and improving decision-making efficiency (Gu et al., 2023). Earlier research has emphasized the importance of precision in fraud detection systems, particularly in banking environments where excessive false positives can disrupt legitimate customer activities and increase operational costs. The current findings aligned with these insights by showing that AI-driven models achieved both higher precision and lower false-positive rates. This improvement was not only statistically significant but also operationally meaningful, as it translated into more efficient allocation of resources and reduced investigation time. The discussion therefore underscored those improvements in detection accuracy must be accompanied by reductions

in false alarms to achieve meaningful gains in cybersecurity performance (Mohamed et al., 2023).

Response time and incident handling efficiency emerged as critical performance indicators in this study, with AI-enhanced SOC systems demonstrating significantly faster detection and response capabilities compared to traditional SIEM systems (Åström et al., 2022). Earlier studies have identified delayed response times as a major vulnerability in cybersecurity operations, particularly in high-risk sectors such as banking, where rapid fraud detection is essential to minimize financial losses. The findings of this study confirmed that AI-driven systems were able to process large volumes of data in real time, enabling quicker identification of anomalies and faster initiation of mitigation actions. Traditional SIEM systems, on the other hand, exhibited longer response times due to reliance on sequential processing and manual intervention. This observation was consistent with prior research that highlighted the limitations of manual workflows in handling high-volume data streams (Y. Zhu et al., 2023). The discussion emphasized that the reduction in response time achieved by AI-enhanced systems represented a significant advancement in operational efficiency, particularly in environments where fraud incidents evolve rapidly. The ability to detect and respond to threats in near real time was identified as a key advantage of AI-driven SOC operations, reinforcing earlier theoretical perspectives on the role of automation and advanced analytics in modern cybersecurity frameworks (George & Wooden, 2023).

The scalability of AI-enhanced SOC systems was another important aspect highlighted in the findings, particularly in comparison to traditional SIEM systems under high data volume conditions. Banking environments generate massive amounts of data from transactions, authentication processes, and system interactions, requiring detection systems to operate efficiently at scale (Damoah et al., 2021). The results showed that AI-enhanced systems maintained stable performance even as data volume and event density increased, whereas SIEM systems experienced performance degradation and increased alert congestion. Earlier studies have pointed out that scalability is a major limitation of rule-based systems, which often struggle to process large datasets without compromising performance. The findings of this study supported these observations by demonstrating that SIEM systems exhibited higher variability in performance metrics under high-load conditions. In contrast, AI-driven systems showed consistent accuracy and efficiency, indicating their ability to scale effectively with increasing data demands (C. Wang et al., 2023). The discussion therefore highlighted that scalability is a critical factor in evaluating the effectiveness of cybersecurity systems, particularly in the context of digital banking, where data volume continues to grow. The ability of AI-enhanced SOC systems to maintain performance under varying conditions was identified as a key strength, supporting their suitability for large-scale deployment (Izhar et al., 2023).

The sub-group analysis provided additional insights into the contextual performance of AI-enhanced SOC systems, particularly in detecting synthetic identity and deepfake-related fraud. The findings indicated that AI-driven systems were particularly effective in identifying synthetic fraud due to their ability to analyze behavioral patterns over time (Regona et al., 2023). Earlier research has emphasized that synthetic identity fraud is characterized by gradual development and subtle anomalies, making it difficult to detect using static rules. The results of this study confirmed that AI-enhanced systems were better equipped to capture these patterns, achieving higher detection accuracy in synthetic fraud scenarios. Similarly, in deepfake-related fraud, AI systems demonstrated superior performance in identifying multimodal anomalies, which involve inconsistencies across different data types such as authentication behavior and transaction patterns (Burrell, 2023). This finding aligned with earlier studies that highlighted the importance of multimodal analysis in detecting advanced fraud techniques. Traditional SIEM systems, which rely on single-dimensional rule-based detection, were less effective in these scenarios, reinforcing the limitations identified in previous research (Votto et al., 2021). The discussion therefore emphasized that the effectiveness of fraud detection systems is highly dependent on their ability to handle complex and multidimensional data, which is a key strength of AI-enhanced SOC operations.

The statistical analysis further strengthened the validity of the findings by demonstrating that the observed differences between AI-enhanced SOC and traditional SIEM systems were not only statistically significant but also practically meaningful. Earlier studies have often reported improvements in AI-based detection systems, but the magnitude of these improvements has not always

been clearly quantified (Ahamad et al., 2022). The present study addressed this gap by providing effect size measurements, which indicated large differences in key performance metrics such as detection accuracy and response time. These results supported earlier theoretical arguments that AI-driven systems offer substantial advantages over rule-based approaches, particularly in dynamic and high-risk environments. The regression analysis also confirmed that system type was a strong predictor of detection performance, further validating the superiority of AI-enhanced SOC operations (Siontis et al., 2021). The discussion highlighted that statistical significance alone is not sufficient to evaluate the effectiveness of a system, and that effect size provides important context regarding the practical impact of the findings. The combination of statistical significance and large effect sizes in this study provided strong evidence that the observed performance differences were both reliable and meaningful in real-world applications (Chen et al., 2022).

The visual representation of findings complemented the statistical analysis by providing clear and intuitive insights into performance trends and distributions. Graphical analysis showed that AI-enhanced SOC systems maintained consistent performance across different time periods and operational conditions, while SIEM systems exhibited greater variability and lower overall performance (Amjad et al., 2023). Earlier research has emphasized the importance of visual analytics in understanding complex data patterns, particularly in cybersecurity, where large datasets and multiple variables can make interpretation challenging. The findings of this study supported this perspective by demonstrating that visual representations helped to highlight key differences between the two systems, including trends in detection accuracy, response time, and alert volume (Johnson, 2019). The discussion emphasized that combining statistical analysis with visual representation provides a more comprehensive understanding of system performance, allowing for both detailed examination and broader interpretation of results. The consistency of AI-enhanced SOC performance across different scenarios further reinforced the conclusions drawn from the statistical analysis, highlighting the robustness and reliability of AI-driven detection systems in banking cybersecurity environments (Madanchian et al., 2023).

CONCLUSION

The discussion of AI-Enhanced Security Operations Center (SOC) operations for deepfake and synthetic fraud detection in banking, in comparison with traditional SIEM systems over the period 2018–2026, demonstrated a clear transformation in cybersecurity effectiveness driven by data-centric intelligence and automation. The findings indicated that AI-enhanced SOC systems consistently outperformed traditional SIEM mechanisms across multiple dimensions, including detection accuracy, response time, error rates, and operational scalability. This study confirmed that rule-based SIEM architectures remained effective in identifying known and structured threat patterns, particularly in conventional fraud scenarios where predefined signatures and correlation rules could be applied reliably. However, performance limitations became evident when addressing complex and adaptive fraud forms such as synthetic identities and deepfake-enabled impersonation, which often evolve beyond static rule thresholds and require contextual interpretation of behavior. The results revealed that AI-driven SOC systems demonstrated significantly higher sensitivity to these evolving threats due to their ability to analyze multidimensional data, recognize behavioral anomalies, and adapt to new fraud patterns over time. In addition, AI-enhanced systems achieved substantial reductions in false-positive and false-negative rates, indicating improved precision and recall in fraud detection. This contributed to more efficient alert management and reduced analyst workload, addressing long-standing concerns related to alert fatigue in traditional SIEM environments. The analysis further showed that response efficiency was significantly improved in AI-based systems, with faster detection and mitigation of threats, which is critical in banking contexts where delays can result in financial losses and reputational damage. Scalability also emerged as a defining advantage of AI-enhanced SOC operations, as these systems maintained stable performance under high data volumes and complex event streams, whereas traditional SIEM systems exhibited performance degradation and increased alert congestion under similar conditions. Sub-group analysis reinforced these findings by demonstrating that AI systems were particularly effective in detecting synthetic fraud through behavioral pattern recognition and deepfake fraud through multimodal anomaly detection, while SIEM systems struggled due to their reliance on static and single-dimensional detection frameworks.

Statistical analysis confirmed that these differences were not only significant but also substantial in magnitude, indicating that the advantages of AI-enhanced SOC systems were both statistically robust and operationally meaningful. Overall, the comparative evaluation highlighted that AI-enhanced SOC operations represent a more adaptive, efficient, and scalable approach to cybersecurity in modern banking environments, particularly in addressing the complexities associated with deepfake and synthetic fraud.

RECOMMENDATIONS

The findings of this study support a set of strategic and operational recommendations for enhancing fraud detection capabilities in banking through the integration of AI-enhanced Security Operations Center (SOC) systems. Financial institutions are advised to progressively transition from purely rule-based SIEM architectures toward hybrid or fully AI-driven SOC environments that incorporate machine learning, behavioral analytics, and automated response mechanisms. This transition should be structured and phased, beginning with the augmentation of existing SIEM systems using AI modules for anomaly detection and alert prioritization, thereby ensuring continuity while improving detection performance. It is also recommended that banks invest in high-quality, diverse, and continuously updated datasets, as the effectiveness of AI models is strongly dependent on data richness and representativeness, particularly in identifying synthetic identity fraud and deepfake-based threats. Additionally, institutions should prioritize the integration of multimodal detection frameworks that combine transactional data, behavioral biometrics, device intelligence, and contextual variables to improve detection accuracy across complex fraud scenarios. The implementation of advanced Security Orchestration, Automation, and Response (SOAR) platforms is further recommended to streamline workflows, reduce response times, and minimize manual intervention, thereby enhancing overall SOC efficiency. Training and upskilling of cybersecurity personnel should also be emphasized, enabling analysts to effectively interpret AI-generated insights and manage automated systems. Furthermore, governance frameworks must be strengthened to address issues related to model transparency, bias, and regulatory compliance, ensuring that AI-based detection systems operate within ethical and legal boundaries. Continuous performance monitoring using standardized metrics such as detection accuracy, error rates, and response efficiency is essential to maintain system reliability and support ongoing optimization. Finally, collaboration across financial institutions and regulatory bodies is recommended to facilitate information sharing, benchmark development, and collective defense against evolving fraud threats. These recommendations collectively highlight the importance of adopting intelligent, scalable, and adaptive SOC frameworks to effectively combat deepfake and synthetic fraud in modern banking environments.

LIMITATION

The study was subject to several limitations that should be acknowledged when interpreting the findings related to AI-enhanced SOC operations and traditional SIEM systems in detecting deepfake and synthetic fraud in banking environments. One primary limitation concerned the reliance on anonymized and partially simulated datasets, which, although carefully constructed and balanced, may not have fully captured the complexity, noise, and unpredictability of real-world banking fraud scenarios. While efforts were made to include diverse fraud types and realistic event sequences, certain emerging fraud tactics, particularly highly sophisticated deepfake attacks, may not have been fully represented due to data availability constraints. Another limitation related to the quasi-experimental design, which did not involve direct manipulation of live banking systems, thereby limiting the ability to observe real-time operational behaviors, system constraints, and human decision-making dynamics under actual conditions. The study also depended on predefined performance metrics such as detection accuracy, false-positive rates, and response time, which, although widely accepted, may not fully encompass all dimensions of cybersecurity effectiveness, such as interpretability, user trust, and long-term system resilience. Additionally, the AI models used in the study were trained and evaluated within controlled environments, and their performance may vary when deployed in heterogeneous banking infrastructures with different data architectures, regulatory requirements, and operational practices. There was also a limitation associated with model generalizability, as the results may be influenced by the specific characteristics of the datasets used, potentially affecting applicability to smaller institutions or regions with different fraud patterns. Furthermore, the comparison with

traditional SIEM systems was based on standardized configurations, which may not reflect the full range of customization and optimization possible in real-world deployments. The temporal scope of the study, covering 2018 to 2026, introduced another constraint, as rapid technological advancements in both AI and fraud techniques could alter system performance beyond the study period. Finally, the study did not fully account for implementation costs, organizational readiness, and integration challenges, which are critical factors in real-world adoption of AI-enhanced SOC systems. These limitations suggest that while the findings provide strong evidence of the advantages of AI-driven detection, caution should be exercised when generalizing the results across different banking contexts and evolving cybersecurity landscapes.

REFERENCES

[1]. Ahamad, S., Mohseni, M., Shekher, V., Smaisim, G. F., Tripathi, A., & Alanya-Beltran, J. (2022). A detailed analysis of the critical role of artificial intelligence in enabling high-performance cloud computing systems. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE),

[2]. Albert, A. (2025). AI-Driven Real-Time Methane Emissions Monitoring and Predictive Leak Detection Using Lidar and IOT Sensor Fusion in Upstream Oil and Gas Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2035–2077. https://doi.org/10.63125/yavd2f86

[3]. Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., Aldairem, A., Alrashed, M., Bin Saleh, K., & Badreldin, H. A. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC medical education*, *23*(1), 689.

[4]. Amena Begum, S., & Mst Kaniz, F. (2023). Advanced Computational and Biotechnological Approaches to Systemic Family Therapy: Predicting Marital Satisfaction and Emotional Wellbeing in Couples. *Review of Applied Science and Technology*, *2*(04), 228–265. https://doi.org/10.63125/4sy9qa21

[5]. Amena Begum, S., & Mst Kaniz, F. (2024). Integrating Psychometric and Neurocognitive Biomarkers in Computational Models to Predict Cognitive Behavioral Therapy Outcomes in Adolescents with Anxiety and Depression. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 632–677. https://doi.org/10.63125/7t7wmp27

[6]. Amjad, A., Kordel, P., & Fernandes, G. (2023). A review on innovation in healthcare sector (telehealth) through artificial intelligence. *Sustainability*, *15*(8), 6655.

[7]. Anick, K. M. T. A. (2025). AI-Enabled Decision Support Systems for Industrial Energy Optimization in U.S. Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2160–2201. https://doi.org/10.63125/8vyhwm46

[8]. Arfaoui, B., Mrabet, H., & Jemai, A. (2023). "SOCaaS-IoT" A Security Operations Center as a Service Approach for IoT Applications Using Open-Source SIEM. 2023 IEEE Afro-Mediterranean Conference on Artificial Intelligence (AMCAI),

[9]. Armellin, A., Gaggero, G. B., Cattelino, A., Piana, L., Raggi, S., & Marchese, M. (2023). Integrating OT data in SIEM platforms: an Energy Utility Perspective. 2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE),

[10]. Åström, J., Reim, W., & Parida, V. (2022). Value creation and value capture for AI business model innovation: a three-phase process framework. *Review of Managerial Science*, *16*(7), 2111-2133.

[11]. Autsadee, Y., Jeevan, J., Mohd Salleh, N. H. B., & Othman, M. R. B. (2023). Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, *7*(4), 2286409.

[12]. Baraheem, S. S., & Nguyen, T. V. (2023). AI vs. AI: Can AI detect AI-generated images? *Journal of Imaging*, *9*(10), 199.

[13]. Barletta, V. S., Caivano, D., Lako, A., & Pal, A. (2023). Quantum as a service architecture for security in a smart city. International Conference on the Quality of Information and Communications Technology,

[14]. Behrooz, H., Lipizzi, C., Korfiatis, G., Ilbeigi, M., Powell, M., & Nouri, M. (2023). Towards automating the identification of sustainable projects seeking financial support: An AI-powered approach. *Sustainability*, *15*(12), 9701.

[15]. Beju, D.-G., & Făt, C.-M. (2023). Frauds in banking system: Frauds with cards and their associated services. In *Economic and financial crime, sustainability and good governance* (pp. 31-52). Springer.

[16]. Benalcazar, D., Tapia, J. E., Gonzalez, S., & Busch, C. (2023). Synthetic id card image generation for improving presentation attack detection. *IEEE Transactions on Information Forensics and Security*, *18*, 1814-1824.

[17]. Berdibayev, R., Gnatyuk, S., Yevchenko, Y., & Kishchenko, V. (2021). A concept of the architecture and creation for siem system in critical infrastructure. In *Systems, Decision and Control in Energy II* (pp. 221-242). Springer.

[18]. Bisht, D., Singh, R., Gehlot, A., Akram, S. V., Singh, A., Montero, E. C., Priyadarshi, N., & Twala, B. (2022). Imperative role of integrating digitalization in the firms finance: A technological perspective. *Electronics*, *11*(19), 3252.

[19]. Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access*, *11*, 69783-69797.

[20]. Bonfanti, M. E. (2022). Artificial intelligence and the offense–defense balance in cyber security. In *Cyber Security Politics* (pp. 64-77). Routledge.

[21]. Bozzano, M., Bussola, R., Cristoforetti, M., Goyal, S., Jonáš, M., Kapellos, K., Micheli, A., Soldà, D., Tonetta, S., & Tranoris, C. (2022). ROBDT: AI-enhanced digital twin for space exploration robotic assets. International Conference on Applied Intelligence and Informatics,

[22]. Bryant, B. D., & Saiedian, H. (2020). Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers & Security*, *94*, 101817.
[23]. Burrell, D. N. (2023). Dynamic evaluation approaches to telehealth technologies and artificial intelligence (AI) telemedicine applications in healthcare and biotechnology organizations. *Merits*, *3*(4), 700-721.
[24]. Burton, J. (2023). Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. *Technology in society*, *75*, 102262.
[25]. Cali, U., Dimd, B. D., Hajialigol, P., Moazami, A., Gourisetti, S. N. G., Lobaccaro, G., & Aghaei, M. (2023). Digital twins: Shaping the future of energy systems and smart cities through cybersecurity, efficiency, and sustainability. 2023 International Conference on Future Energy Solutions (FES),
[26]. Chaithanya, B., & Brahmananda, S. (2022). AI-enhanced defense against ransomware within the organization's architecture. *Journal of Cyber Security and Mobility*, *11*(4), 621-654.
[27]. Chen, X., Tao, X., Wang, F. L., & Xie, H. (2022). Global research on artificial intelligence-enhanced human electroencephalogram analysis. *Neural Computing and Applications*, *34*(14), 11295-11333.
[28]. Chen, Y., Wesemann, S., & Wild, T. (2023). Turbo AI, Part V: Verifying AI-Enhanced Channel Estimation for RAN from System Level. 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),
[29]. Choi, I., Lee, J., Kwon, T., Kim, K., Choi, Y., & Song, J. (2021). An easy-to-use framework to build and operate ai-based intrusion detection for in-situ monitoring. 2021 16th Asia joint conference on information security (AsiaJCIS),
[30]. Christian, J., Paulino, L., & de Sá, A. O. (2022). A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response. International Conference on Information Security Practice and Experience,
[31]. Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety*, *24*(1), 30-41.
[32]. Damoah, I. S., Ayakwah, A., & Tingbani, I. (2021). Artificial intelligence (AI)-enhanced medical drones in the healthcare supply chain (HSC) for sustainability development: A case study. *Journal of Cleaner Production*, *328*, 129598.
[33]. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920.
[34]. de la Rosa, J. M. (2022). AI-managed cognitive radio digitizers. *IEEE Circuits and Systems Magazine*, *22*(1), 10-39.
[35]. De Ruiter, A. (2021). The distinct wrong of deepfakes. *Philosophy & Technology*, *34*(4), 1311-1332.
[36]. Demircioglu, P., Bogrekci, I., Durakbasa, M. N., & Bauer, J. (2023). Autonomation, automation, AI, and industry-agriculture 5.0 in sustainable agro-ecological food production. The International Symposium for Production Research,
[37]. Dimitrov, W., Dimitrov, G., Spasov, K., & Syarova, S. (2021). Conceptual model for a shared cybersecurity operations center for ICS. In *Proceedings of the Computational Methods in Systems and Software* (pp. 493-503). Springer.
[38]. Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking cybercrime with artificial-intelligence-driven cybersecurity analytics. *Sensors*, *23*(14), 6302.
[39]. Doynikova, E., Fedorchenko, A., & Kotenko, I. (2020). A semantic model for security evaluation of information systems. *Journal of Cyber Security and Mobility*, *9*(2), 301-330.
[40]. El Hajj, M., & Hammoud, J. (2023). 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*, *16*(10), 434.
[41]. Eriksson, H. S., & Grov, G. (2022). Towards XAI in the SOC–a user centric study of explainable alerts with SHAP and LIME. 2022 IEEE international conference on big data (Big Data),
[42]. Esseghir, A., Kamoun, F., & Hraiech, O. (2022). AKER: An open-source security platform integrating IDS and SIEM functions with encrypted traffic analytic capability. *Journal of Cyber Security Technology*, *6*(1-2), 27-64.
[43]. Fatima, S., Desouza, K. C., & Dawson, G. S. (2020). National strategic artificial intelligence plans: A multi-dimensional analysis. *Economic Analysis and Policy*, *67*, 178-194.
[44]. Ferdous Ara, A., & Beatrice Onyinyechi, M. (2023). Long-Term Epidemiologic Trends of STIs PRE- and post-PrEP Introduction: A National Time-Series Analysis. *American Journal of Health and Medical Sciences*, *4*(02), 01–35. https://doi.org/10.63125/mp153d97
[45]. Fuentes-García, M., Camacho, J., & Maciá-Fernández, G. (2021). Present and future of network security monitoring. *IEEE Access*, *9*, 112744-112760.
[46]. Garde, A., Suratkar, S., & Kazi, F. (2022). AI based deepfake detection. 2022 IEEE 1st International Conference on Data, Decision and Systems (ICDDS),
[47]. Gaur, L., Mallik, S., & Jhanjhi, N. Z. (2022). Introduction to deepfake technologies. In *DeepFakes* (pp. 1-8). CRC Press.
[48]. Gautam, V., Joshi, M., Tiwari, R. G., Agarwal, A. K., & Trivedi, N. K. (2023). A performance analysis to detect synthetic images with deep learning-based image classification. International Conference on Cyber Intelligence and Information Retrieval,
[49]. George, B., & Wooden, O. (2023). Managing the strategic transformation of higher education through artificial intelligence. *Administrative Sciences*, *13*(9), 196.
[50]. Ghaleb, F. A., Maarof, M. A., Zainal, A., Al-Rimy, B. A. S., Saeed, F., & Al-Hadhrami, T. (2019). Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network. *IEEE Access*, *7*, 159119-159140.
[51]. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

[52]. Gu, H., Zhao, L., Han, Z., Zheng, G., & Song, S. (2023). AI-enhanced cloud-edge-terminal collaborative network: Survey, applications, and future directions. *IEEE Communications Surveys & Tutorials*, *26*(2), 1322-1385.
[53]. Hairab, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2022). Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks. *IEEE Access*, *10*, 98427-98440.
[54]. Hasan, K., Shetty, S., & Ullah, S. (2019). Artificial intelligence empowered cyber threat detection and protection for power utilities. 2019 IEEE 5th international conference on collaboration and internet computing (CIC),
[55]. Hata, M. B. M., Darus, M. Y. B., Shafiee, M. Z. A. B., Petrus, E., & Jamian, Y. A. (2023). A log aggregation design criteria for robust SIEM (security information and event management) in enhancing threat detection. 2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE),
[56]. Helkala, K., Cook, J., Lucas, G., Pasquale, F., Reichberg, G., & Syse, H. (2022). AI in cyber operations: ethical and legal considerations for end-users. In *Artificial Intelligence and Cybersecurity: Theory and Applications* (pp. 185-206). Springer.
[57]. Hisham, M., & Khairum Nahar, P. (2024). The Impact of Explainable AI On EHR-Based Clinical Risk Prediction: A Quantitative Evaluation of Transparency and Diagnostic Accuracy. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 593–631. https://doi.org/10.63125/vepxg976
[58]. Islam, C., Babar, M. A., & Nepal, S. (2020). Architecture-centric support for integrating security tools in a security orchestration platform. European Conference on Software Architecture,
[59]. Islam, M. D. Z., & Aditya, D. (2023). Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE + AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), 01-42. https://doi.org/10.63125/8ycz7671
[60]. Istiaq, A., & Tanjina Binte, S. (2023). AI-Driven Vulnerability Prioritization for Enterprise Networks: A Quantitative Study Using Attack-Graph Models. *American Journal of Advanced Technology and Engineering Solutions*, *3*(04), 129-166. https://doi.org/10.63125/s6qn2t38
[61]. Izhar, M., Naqvi, S. A. A., Ahmed, A., Abdullah, S., Alturki, N., & Jamel, L. (2023). Enhancing healthcare efficacy through IoT-edge fusion: A novel approach for smart health monitoring and diagnosis. *IEEE Access*, *11*, 136456-136467.
[62]. Johnson, J. (2019). The AI-cyber nexus: implications for military escalation, deterrence and strategic stability. *Journal of cyber policy*, *4*(3), 442-460.
[63]. Johnson, J., Jones, C. B., Chavez, A., & Hossain-McKenzie, S. (2023). Soar4der: security orchestration, automation, and response for distributed energy resources. In *Power Systems Cybersecurity: Methods, Concepts, and Best Practices* (pp. 387-411). Springer.
[64]. Kazi Rakib Hasan, S. (2025). Quantitative Evaluation of Machine Learning Models for Project Risk Prediction and Resource Optimization in Business Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2119–2159. https://doi.org/10.63125/01bg6n62
[65]. KHetsuriani, E., Bondarenko, V., Surzhko, O., KHetsuriani, T., & Asatryan, A. (2023). Conceptual Foundations of Methodology in the Creation and Development of a Class of Natural-Technical Systems. International Conference on Construction, Architecture and Technosphere Safety,
[66]. Kingra, S., Aggarwal, N., & Kaur, N. (2023). Emergence of deepfakes and video tampering detection approaches: A survey. *Multimedia Tools and Applications*, *82*(7), 10165-10209.
[67]. Kitsios, F., Kamariotou, M., Syngelakis, A. I., & Talias, M. A. (2023). Recent advances of artificial intelligence in healthcare: a systematic literature review. *Applied sciences*, *13*(13), 7479.
[68]. Kovačević, I., Groš, S., & Slovenec, K. (2020). Systematic review and quantitative comparison of cyberattack scenario detection and projection. *Electronics*, *9*(10), 1722.
[69]. Kwok, A. O., & Koh, S. G. (2021). Deepfake: a social construction of technology perspective. *Current Issues in Tourism*, *24*(13), 1798-1802.
[70]. Laas, O. (2023). Deepfakes and trust in technology. *Synthese*, *202*(5), 132.
[71]. Langevin, A., Cody, T., Adams, S., & Beling, P. (2022). Generative adversarial networks for data augmentation and transfer in credit card fraud detection. *Journal of the Operational Research Society*, *73*(1), 153-180.
[72]. Lee, S., & Huh, J.-H. (2019). An effective security measures for nuclear power plant using big data analysis approach: S. Lee, J.-H. Huh. *The Journal of Supercomputing*, *75*(8), 4267-4294.
[73]. López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*, *22*(3), 691-711.
[74]. Lu, Y. (2019). Artificial intelligence: a survey on evolution, models, applications and future trends. *Journal of management analytics*, *6*(1), 1-29.
[75]. Lyu, S. (2022). Deepfake detection. In *Multimedia forensics* (pp. 313-331). Springer.
[76]. Madanchian, M., Taherdoost, H., & Mohamed, N. (2023). AI-based human resource management tools and techniques; a systematic literature review. *Procedia Computer Science*, *229*, 367-377.
[77]. Mahfuj Ahmed, R. (2024). IoT-Driven Digital Transformation in Global Supply Chains: Implications for Financial Risk Monitoring and Investment Efficiency. *American Journal of Scholarly Research and Innovation*, *3*(02), 375–421. https://doi.org/10.63125/7ywwk960
[78]. Majeed, A., ur Rasool, R., Ahmad, F., Alam, M., & Javaid, N. (2019). Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. *Journal of Ambient Intelligence and Humanized Computing*, *10*(4), 1509-1526.
[79]. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward: Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward. *Applied intelligence*, *53*(4), 3974-4026.

[80]. Mayer, R., Hittmeir, M., & Ekelhart, A. (2020). Privacy-preserving anomaly detection using synthetic data. IFIP Annual Conference on Data and Applications Security and Privacy,

[81]. Md, F. (2023). A Review on Understanding Data Governance Failures in Analytics Systems: Insights from Expert Interviews and Root-Cause Thematic Coding. *Journal of Sustainable Development and Policy*, *2*(04), 346-385. https://doi.org/10.63125/rem5kx95

[82]. Md Khaled, H. (2021). An Empirical Study of CRM and Analytics-Based Approaches to Customer Engagement and Sales Performance Evaluation in Enterprise Organizations. *American Journal of Data Science and Analytics*, *2*(12), 76-155. https://doi.org/10.63125/1tt57n77

[83]. Md Khaled, H., & Hisham, M. (2022). Intelligent Decision-Support Systems for Cross-Functional Workflow Optimization in Data-Driven Organizations. *Journal of Sustainable Development and Policy*, *1*(02), 168-207. https://doi.org/10.63125/dsfg3k24

[84]. Md. Ashfaq, S., & Ashraful, I. (2025). Quantitative Analysis of Machine Learning Models For Defect Prediction in Metal Additive Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1810–1847. https://doi.org/10.63125/3fkkwg05

[85]. Md. Nazmul, H., & Amena Begum, S. (2022). AI-Based Psychodiagnostics' Models to Support Early Intervention and Reduce Suicide Risk in Adolescents and Youth: Development and Clinical Validation. *American Journal of Data Science and Analytics*, *3*(06), 40-79. https://doi.org/10.63125/vb5f7e98

[86]. Md. Shahinur, I., & Md. Sultan, M. (2022). Digital-Twin-Based Quantitative Frameworks for Modeling, Monitoring, and Optimization of Electrical Power Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 365-393. https://doi.org/10.63125/dvmj1y93

[87]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06

[88]. Mir, A. W., & Ramachandran, R. K. (2021). Implementation of security orchestration, automation and response (SOAR) in smart grid-based SCADA systems. Sixth International Conference on Intelligent Computing and Applications: Proceedings of ICICA 2020,

[89]. Mohamed, N., Ahmed, A. A., Alsharif, A., & ElKhozondar, H. J. (2023). Employing AI-driven drones and advanced cyber penetration tools for breakthrough criminal network surveillance. 2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE),

[90]. Mojarad, R., Attal, F., Chibani, A., & Amirat, Y. (2020a). A context-aware approach to detect abnormal human behaviors. Joint European Conference on Machine Learning and Knowledge Discovery in Databases,

[91]. Mojarad, R., Attal, F., Chibani, A., & Amirat, Y. (2020b). A context-aware hybrid framework for human behavior analysis. 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI),

[92]. Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Springer.

[93]. Mubarak, R., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2023). A survey on the detection and impacts of deepfakes in visual, audio, and textual formats. *IEEE Access*, *11*, 144497-144529.

[94]. Mukta, M. S. H., Ahmad, J., Raiaan, M. A. K., Islam, S., Azam, S., Ali, M. E., & Jonkman, M. (2023). An investigation of the effectiveness of deepfake models and tools. *Journal of sensor and actuator networks*, *12*(4), 61.

[95]. Murad, M. D. H. R. (2025). Machine Learning–Based Consumer Behavior Prediction Models for E-Commerce Platforms: Enhancing Digital Financial Inclusion and Market Accessibility. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2078–2118. https://doi.org/10.63125/pnz32s94

[96]. Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. *Big Data and Cognitive Computing*, *7*(2), 93.

[97]. Najafi, P., Cheng, F., & Meinel, C. (2021). SIEMA: bringing advanced analytics to legacy security information and event management. International Conference on Security and Privacy in Communication Systems,

[98]. Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476.

[99]. Oliveira, J. S., Souza, G. B., Rocha, A. R., Deus, F. E., & Marana, A. N. (2020). Cross-domain deep face matching for real banking security systems. 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG),

[100]. Oliveri, G., Zardi, F., Rocca, P., Salucci, M., & Massa, A. (2022). Building a smart EM environment-AI-Enhanced aperiodic micro-scale design of passive EM skins. *IEEE Transactions on Antennas and Propagation*, *70*(10), 8757-8770.

[101]. Onwubiko, C., & Ouazzane, K. (2019). Cyber onboarding is 'broken'. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),

[102]. Orsós, M., Kecskés, M., Kail, E., & Bánáti, A. (2022). Log collection and SIEM for 5G SOC. 2022 IEEE 20th jubilee world symposium on applied machine intelligence and informatics (SAMI),

[103]. Pan, Z., Hariri, S., & Pacheco, J. (2019). Context aware intrusion detection for building automation systems. *Computers & Security*, *85*, 181-201.

[104]. Pashentsev, E. (2023). The malicious use of deepfakes against psychological security and political stability. In *The Palgrave handbook of malicious use of AI and psychological security* (pp. 47-80). Springer.

[105]. Patel, Y., Tanwar, S., Gupta, R., Bhattacharya, P., Davidson, I. E., Nyameko, R., Aluvala, S., & Vimal, V. (2023). Deepfake generation and detection: Case study and challenges. *IEEE Access*, *11*, 143296-143323.

[106]. Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital society*, *1*(2), 19.

[107]. Pitropakis, N., Logothetis, M., Andrienko, G., Stefanatos, J., Karapistoli, E., & Lambrinoudakis, C. (2019). Towards the creation of a threat intelligence framework for maritime infrastructures. International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems,

[108]. Podzins, O., & Romanovs, A. (2019). Why siem is irreplaceable in a secure it environment? 2019 open conference of electrical, electronic and information sciences (eStream),

[109]. Raj, M. T., Arunachalam, M., Ramalakshmi, R., Ramaraj, K., Arunachalam, M., & Kaleeswari, P. (2023). A review on the detection of deep fake and propaganda videos and images-based voice and facial manipulation using AI techniques. 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS),

[110]. Rajib, S. (2024). Quantitative Assessment of Data-Driven Pricing Optimization Strategies for E-Commerce Platforms in Developing Economies. *Review of Applied Science and Technology*, *3*(02), 01–40. https://doi.org/10.63125/g5va6e03

[111]. Regona, M., Yigitcanlar, T., Hon, C. K., & Teo, M. (2023). Mapping two decades of AI in construction research: A scientometric analysis from the sustainability and construction phases lenses. *Buildings*, *13*(9), 2346.

[112]. Rojek, I., Jasiulewicz-Kaczmarek, M., Piechowski, M., & Mikołajewski, D. (2023). An artificial intelligence approach for improving maintenance to supervise machine failures and support their repair. *Applied sciences*, *13*(8), 4971.

[113]. Rukaiya Khatun, M., & Zakia, A. (2023). Quantitative Assessment of Data Privacy and Access Control Effectiveness in SAP/ERP Analytics Systems. *Review of Applied Science and Technology*, *2*(01), 259–300. https://doi.org/10.63125/vb03b363

[114]. Santoso, F., & Finn, A. (2023). An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. *IEEE Transactions on Services Computing*, *17*(3), 1293-1310.

[115]. Saraiva, M., & Mateus-Coelho, N. (2022). CyberSoc framework a systematic review of the state-of-art. *Procedia Computer Science*, *204*, 961-972.

[116]. Sareen, M. (2022). Threats and challenges by DeepFake technology. In *DeepFakes* (pp. 99-113). CRC Press.

[117]. Sarker, I. H., Colman, A., Han, J., Khan, A. I., Abushark, Y. B., & Salah, K. (2020). Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model. *Mobile Networks and Applications*, *25*(3), 1151-1161.

[118]. Sarker, I. H., Colman, A., Han, J., & Watters, P. (2021). Introduction to context-aware machine learning and mobile data analytics. In *Context-Aware Machine Learning and Mobile Data Analytics: Automated Rule-based Services with Intelligent Decision-Making* (pp. 3-13). Springer.

[119]. Sarker, I. H., & Kayes, A. (2020). ABC-RuleMiner: User behavioral rule-based machine learning method for context-aware intelligent services. *Journal of Network and Computer Applications*, *168*, 102762.

[120]. Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 41.

[121]. Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525-2556.

[122]. Sebbar, A., Cherqi, O., Chougdali, K., & Boulmalf, M. (2023). Real-time anomaly detection in SDN architecture using integrated SIEM and machine learning for enhancing network security. GLOBECOM 2023-2023 IEEE Global Communications Conference,

[123]. Sen, Ö., van der Velde, D., Wehrmeister, K. A., Hacker, I., Henze, M., & Andres, M. (2021). Towards an approach to contextual detection of multi-stage cyber attacks in smart grids. 2021 International Conference on Smart Energy Systems and Technologies (SEST),

[124]. Shahjee, D., & Ware, N. (2022). Integrated network and security operation center: A systematic analysis. *IEEE Access*, *10*, 27881-27898.

[125]. Shamsul, A. (2025). AI-Driven Condition Monitoring and Fault Detection in Electrical Power and Industrial Control Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1778–1809. https://doi.org/10.63125/csjs7238

[126]. Shamsul, A., & Md. Morshedul, I. (2025). The Role of Cloud-Native Infrastructures in Supporting Autonomous and Uncrewed Systems (UXS) in Operations. *Journal of Sustainable Development and Policy*, *4*(03), 82-125. https://doi.org/10.63125/vntbqq40

[127]. Sharma, M., & Kaur, M. (2021). A review of Deepfake technology: an emerging AI threat. *Soft Computing for Security Applications: Proceedings of ICSCS 2021*, 605-619.

[128]. Shi, D., Zhao, J., Eze, C., Wang, Z., Wang, J., Lian, Y., & Burke, A. F. (2023). Cloud-based artificial intelligence framework for battery management system. *Energies*, *16*(11), 4403.

[129]. Shoaib, M. R., Wang, Z., Ahvanooey, M. T., & Zhao, J. (2023). Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models. 2023 international conference on computer and applications (ICCA),

[130]. Sikder, A. K., Aksu, H., & Uluagac, A. S. (2019). A context-aware framework for detecting sensor-based threats on smart devices. *IEEE Transactions on Mobile Computing*, *19*(2), 245-261.

[131]. Siontis, K. C., Noseworthy, P. A., Attia, Z. I., & Friedman, P. A. (2021). Artificial intelligence-enhanced electrocardiography in cardiovascular disease management. *Nature Reviews Cardiology*, *18*(7), 465-478.

[132]. Stecuła, K., Wolniak, R., & Grebski, W. W. (2023). AI-Driven urban energy solutions—from individuals to society: a review. *Energies*, *16*(24), 7988.

[133]. Tahmina Akter Bhuya, M. (2025). Machine Learning-Driven Credit Risk Modeling: Transforming Loan Default Prediction and Portfolio Management in U.S. Commercial Banking. *American Journal of Data Science and Analytics*, *6*(12), 01-42. https://doi.org/10.63125/0z894070

[134]. Tanjina Binte, S., & Md. Hasan Or, R. (2022). Advanced Computing, IT Strategy, and Network-Optimized Frameworks for Retail Business Intelligence. *American Journal of Interdisciplinary Studies*, *3*(04), 429-463. https://doi.org/10.63125/dgyg3762

[135]. Tanjina Binte, S., & Sazzadul, I. (2022). Advanced Financial Data Analytics for Anomaly Detection and Pattern Discovery in Large-Scale Financial Data Pipelines. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 174-210. https://doi.org/10.63125/g1cdm484

[136]. Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach. *Applied sciences*, *13*(22), 12359.

[137]. Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A roadmap for SMEs to adopt an AI based cyber threat intelligence. In *The effect of information technology on business and marketing intelligence systems* (pp. 1903-1926). Springer.

[138]. Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, *8*, 227756-227779.

[139]. Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., & Pernul, G. (2021). A digital twin-based cyber range for SOC analysts. IFIP Annual Conference on Data and Applications Security and Privacy,

[140]. Vielberth, M., Menges, F., & Pernul, G. (2019). Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity*, *2*(1), 23.

[141]. Vignesh Saravanan, K., Jothi Thilaga, P., Kavipriya, S., & Vijayalakshmi, K. (2023). Data protection and security enhancement in cyber-physical systems using AI and blockchain. In *AI models for blockchain-based intelligent networks in IoT systems: Concepts, Methodologies, tools, and applications* (pp. 285-325). Springer.

[142]. Villalón-Huerta, A., Gisbert, H. M., & Ripoll-Ripoll, I. (2022). SOC critical path: A defensive kill chain model. *IEEE Access*, *10*, 13570-13581.

[143]. Votto, A. M., Valecha, R., Najafirad, P., & Rao, H. R. (2021). Artificial intelligence in tactical human resource management: A systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100047.

[144]. Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Springer.

[145]. Wang, C., He, T., Zhou, H., Zhang, Z., & Lee, C. (2023). Artificial intelligence enhanced sensors-enabling technologies to next-generation healthcare and biomedical platform. *Bioelectronic Medicine*, *9*(1), 17.

[146]. Wang, J., Zhang, L., Yang, Y., Zhuang, Z., Qi, Q., Sun, H., Lu, L., Feng, J., & Liao, J. (2023). Network meets ChatGPT: Intent autonomous management, control and operation. *Journal of Communications and Information Networks*, *8*(3), 239-255.

[147]. Wang, L., Liu, Z., Liu, A., & Tao, F. (2021). Artificial intelligence in product lifecycle management. *The International Journal of Advanced Manufacturing Technology*, *114*(3), 771-796.

[148]. Whyte, C. (2020a). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of cyber policy*, *5*(2), 199-217.

[149]. Whyte, C. (2020b). Problems of poison: new paradigms and" agreed" competition in the era of AI-enabled cyber operations. 2020 12th International conference on cyber conflict (CyCon),

[150]. Yeng, P. K., Nweke, L. O., Woldaregay, A. Z., Yang, B., & Snekkenes, E. A. (2020). Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. Proceedings of SAI Intelligent Systems Conference,

[151]. Zaheda, K. (2021). Design and Optimization of Dual-Band Microstrip Patch Antenna For 5g Sub-6GHz and mmWave Applications. *American Journal of Data Science and Analytics*, *2*(12), 41-75. https://doi.org/10.63125/cnze8c43

[152]. Zakia, A., & Rukaiya Khatun, M. (2024). Quantitative Assessment of CRM-Based Business Intelligence on Customer Satisfaction and Retention: Evidence from Multi-Channel Service Operations. *Journal of Sustainable Development and Policy*, *3*(02), 01-42. https://doi.org/10.63125/hjd22x72

[153]. Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). Towards IoT security automation and orchestration. 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),

[154]. Zhu, N., Liu, Y., Zhang, J., & Wang, N. (2023). Contingent reward versus punishment and compliance behavior: the mediating role of affective attitude and the moderating role of operational capabilities of artificial intelligence. *Humanities and Social Sciences Communications*, *10*(1), 590.

[155]. Zhu, Y., Wang, T., Wang, C., Quan, W., & Tang, M. (2023). Complexity-driven trust dynamics in human–robot interactions: Insights from ai-enhanced collaborative engagements. *Applied sciences*, *13*(24), 12989.