AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

FEDERATED LEARNING FOR CYBER THREAT DETECTION IN DIGITAL BANKING SYSTEMS

Majoju Sridhar Kumar, VU Research scholor, Mail id: sridharmsk@gmail.com, mobile:9000099402.

Abstract

This research explores Federated Learning for cyber threat detection in digital banking systems using secondary qualitative data analysis. Literature review reveals that FL enables collaborative, privacy-preserving model training across distributed banking nodes, enhancing detection of malware, phishing, and transactional anomalies. Key themes identified include applications of FL in cybersecurity, benefits and limitations, and operational implementation strategies. Findings indicate that FL improves privacy, regulatory compliance, and threat intelligence but faces challenges such as data heterogeneity, communication latency, and interpretability. The study emphasizes the importance of adaptive strategies, secure aggregation, and phased deployment to maximize effectiveness and informs future research on empirical validation and cross-institution collaboration.

Keywords: Federated Learning, Cyber Threat Detection, Digital Banking, Data Privacy, Machine Learning, Financial Security, Intrusion Detection

I. INTRODUCTION

Digital banking systems have become increasingly sophisticated, enabling convenient financial transactions but simultaneously presenting significant cybersecurity challenges. Cyber threats, including phishing attacks, malware, ransomware, and unauthorized access, continue to grow in scale and sophistication [1]. Traditional centralized cybersecurity solutions often struggle to cope with these evolving threats due to limitations in data sharing, privacy concerns, and latency in threat detection. Consequently, banking institutions seek innovative approaches to enhance security without compromising sensitive customer data.

Federated Learning (FL) emerges as a promising paradigm in this context, offering distributed machine learning while preserving data privacy. By enabling multiple banks or branches to collaboratively train models without sharing raw data, FL can detect patterns of cyber threats effectively [2]. This research investigates how FL can be utilized for cyber threat detection in digital banking systems by synthesizing insights from existing literature, identifying best practices, and uncovering gaps in current methodologies.

Problem Statement

Digital banking systems are increasingly targeted by sophisticated cyber attacks, resulting in financial losses, reputational damage, and regulatory challenges. Traditional centralized machine learning models require aggregating sensitive financial data, raising privacy concerns and compliance risks under regulations like GDPR and PCI DSS [3]. Additionally, centralization creates single points of failure, delaying threat detection and response. Existing security frameworks often fail to integrate distributed threat intelligence effectively, limiting their ability to anticipate evolving attack patterns. There is a critical need for privacy-preserving, collaborative learning methods that can detect cyber threats in real time across multiple banking systems [4]. Federated Learning addresses this need by allowing decentralized model training while keeping sensitive data localized. However, research on its practical implementation for cyber threat detection in banking remains fragmented, necessitating a comprehensive review of current methodologies, evaluation strategies, and technological barriers to inform future deployments.

Aims and Objectives

The aim of the research is to explore the effectiveness of Federated Learning in detecting cyber threats in digital banking

systems using secondary qualitative data analysis.

1. To identify the current applications of Federated Learning in cybersecurity for digital banking.
2. To evaluate the benefits and limitations of using Federated Learning for cyber threat detection.
3. To provide recommendations for integrating Federated Learning into existing digital banking security frameworks.

II. LITERATURE REVIEW

Fig 1: Flow of the Review

Structured Literature Review Approach followed the following steps:

I. Identification of relevant academic databases and sources to gather peer-reviewed articles.
II. Systematic search, selection, and critical appraisal of studies relevant to Federated Learning and cybersecurity in banking.
III. Synthesis of findings to identify trends, technological gaps, and practical challenges.

Academic Database and Source Utilization for this study are:

I. Scopus, Web of Science, and IEEE Xplore for peer-reviewed academic articles.
II. ACM Digital Library for computing-focused research on Federated Learning.
III. Google Scholar for supplementary studies and reports on digital banking cybersecurity.

A. Searching Study:

The study conducts a systematic search for literature addressing Federated Learning applications in cybersecurity, specifically within digital banking. Keywords such as "federated learning," "cyber threat detection," "digital banking security," and "distributed machine learning" are used. Boolean operators refine searches, combining concepts of privacy, threat detection, and financial systems. Studies from 2018 to 2025 are prioritized to reflect the latest advancements. Both theoretical frameworks and empirical studies are considered to ensure a comprehensive understanding. This process enables identification of studies that highlight model architectures, performance metrics, collaborative learning approaches, and privacy-preserving mechanisms relevant to banking cyber threat detection.

B. Selection of Journal Articles:

Articles are selected based on relevance, citation impact, and methodological rigor. Peer-reviewed journals and conference proceedings that address Federated Learning, cybersecurity in financial institutions, and intrusion detection systems are prioritized. Non-relevant studies, duplicate records, and articles without empirical or conceptual contributions are excluded. Quality appraisal considers clarity of objectives, research methodology, and relevance to digital banking environments. Selected articles cover both technical aspects, such as model optimization and performance evaluation, and applied contexts, including implementation challenges in banking systems. This selection ensures that only authoritative, high-quality studies contribute to the synthesis and analysis of findings.

C. The Goal of the Review:

The literature review aims to synthesize existing knowledge on Federated Learning for cyber threat detection, identify trends, and assess practical applications in digital banking. It seeks to map the evolution of FL techniques, privacy-preserving mechanisms, and cybersecurity strategies. Additionally, the

review examines the effectiveness, scalability, and limitations of FL implementations. By evaluating previous studies, the review highlights knowledge gaps and technological barriers. The ultimate goal is to provide evidence-based insights for financial institutions seeking to adopt FL frameworks, offering recommendations for model selection, implementation strategies, and integration with existing security infrastructure to enhance threat detection and data privacy.

D. Study of Previous Literature

1. Federated Learning in Cybersecurity:

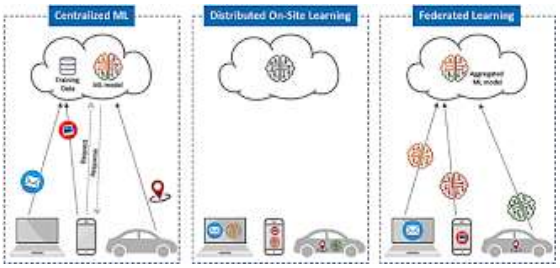

Fig 2: Concept of Federal Learning

Federated Learning (FL) has emerged as a transformative paradigm in modern cybersecurity, enabling collaborative model development across distributed systems while maintaining data privacy and confidentiality. As illustrated in *Fig. 2: Concept of Federated Learning*, this approach eliminates the need to transfer raw data from individual clients or nodes to a central server. Instead, each participant trains a local model on its own data and only shares the model parameters or gradients, which are aggregated centrally to form a global model [5].

In the field of cybersecurity, FL has shown significant promise for detecting malware, phishing attacks, and intrusion attempts. This is particularly crucial in environments such as digital banking, where vast amounts of sensitive user data are distributed across multiple branches or financial institutions. Federated models enable **collective intelligence** allowing banks to strengthen their cyber threat detection capabilities without compromising regulatory requirements for data privacy. Studies reveal that FL can achieve **comparable accuracy and detection rates** to centralized models while substantially reducing risks associated with data exposure and breaches.

Nevertheless, FL implementation is not without its technical challenges. Communication overhead remains a major bottleneck, as continuous parameter exchanges between clients and servers can result in high network latency and synchronization issues. Moreover, **heterogeneous data distribution**—where different nodes possess varying data quality, formats, or feature spaces—often leads to slow model convergence and inconsistent performance across participants. To mitigate these issues, techniques such as **secure aggregation**, **differential privacy**, and **encrypted model updates** have been introduced. Secure aggregation ensures that individual model contributions remain confidential even during parameter transmission, while differential privacy injects controlled noise into gradients to obscure sensitive patterns.

In digital banking contexts, FL allows multiple institutions or subsidiaries to **collaboratively train intrusion detection models** while adhering to data protection laws such as GDPR and PCI DSS. Empirical research demonstrates that federated architectures can support distributed threat intelligence sharing, thereby enabling earlier and more precise identification of cyber anomalies. However, scholars emphasize the need for **standardized communication protocols**, efficient optimization algorithms, and **adaptive aggregation strategies** to facilitate real-time cyber threat monitoring and response across decentralized networks [6].

2. Cyber Threat Detection in Digital Banking:

Digital banking systems represent some of the most **high-value targets** for cybercriminals due to their extensive use of sensitive personal and financial information. These systems are susceptible to a wide range of cyber threats including **malware injections, phishing campaigns, insider attacks, and financial fraud**. Traditionally, banks have relied on **centralized machine learning models** that

aggregate customer and transaction data into a single repository to detect anomalies or malicious behavior. While effective, this approach raises significant **privacy, compliance, and security concerns**, particularly in jurisdictions governed by strict data protection laws [7].

Recent advancements advocate for **distributed learning architectures** such as Federated Learning, which mitigate these privacy issues while maintaining or even enhancing threat detection accuracy. Comparative studies between FL and centralized models indicate that FL not only preserves data sovereignty but also improves the system's ability to identify **previously unseen or emerging threats**. This is achieved through collaborative learning, where multiple institutions contribute local model updates derived from unique datasets, thereby enriching the global model's understanding of diverse threat landscapes [8].

The integration of FL with **real-time monitoring systems** further enhances detection capabilities. For instance, digital banking networks can deploy FL-based models on edge servers or secure gateways that analyze transaction behavior in real time, flagging anomalies immediately without transferring sensitive data. However, achieving this level of responsiveness introduces challenges in **model synchronization, latency management, and data imbalance correction**. Many banks encounter highly skewed datasets, where legitimate transactions vastly outnumber fraudulent ones. Consequently, FL models must employ **data balancing techniques**, such as federated oversampling or adaptive weighting, to ensure that minority attack instances are not overlooked.

Operational challenges also persist in ensuring low-latency performance across **high-traffic financial networks**. Given that real-time fraud prevention systems demand decisions within milliseconds, optimization of FL communication and aggregation processes is critical. Thus, digital banks are increasingly investing in hybrid frameworks that combine **edge computing and federated learning**, enabling near-instantaneous threat recognition while ensuring privacy and regulatory compliance.

3. Privacy-Preserving Machine Learning Techniques:

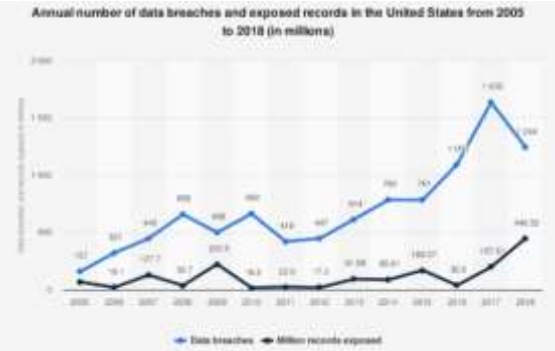

Fig 3: Privacy-Preserving Machine Learning Annual Report

Privacy preservation remains a central challenge in the deployment of machine learning models within financial systems. The financial industry is subject to stringent data protection regulations, including the **General Data Protection Regulation (GDPR)** and regional cybersecurity acts, which restrict data sharing across entities. Federated Learning inherently aligns with these regulations by keeping data localized while still enabling collaborative model improvement [9].

FL leverages several **privacy-preserving techniques** to enhance security during collaborative training. Among the most prominent are **homomorphic encryption**, **differential privacy**, and **secure multi-party computation (SMPC)** [10]. Homomorphic encryption allows computations to be performed on encrypted data, ensuring that even the coordinating server cannot access the raw input. Differential privacy introduces random noise into shared parameters to prevent reverse-engineering of sensitive information, while SMPC ensures that data owners can jointly compute model updates without exposing their individual datasets. Together, these methods safeguard customer confidentiality and minimize the risk of **data leakage** during the learning process.

Studies demonstrate that **privacy-preserving federated models** maintain high levels of detection accuracy comparable to or slightly below that of traditional centralized models while fully complying with financial privacy mandates [11]. However, these techniques introduce computational and communication overhead. Balancing the **trade-offs between privacy protection, model accuracy, and resource efficiency** is therefore a crucial consideration for practical implementation. Excessive encryption or differential privacy noise can degrade detection precision, whereas relaxed privacy measures may expose sensitive data to inference attacks.

Moreover, privacy preservation enhances not only regulatory compliance but also **customer trust and institutional reputation** [12]. Financial clients are more likely to engage with digital banking services that prioritize data security and transparency. As such, privacy-preserving FL approaches have become a cornerstone for **responsible AI adoption** in financial cybersecurity, enabling secure collaboration across distributed banking networks while fostering confidence in data-driven threat prevention systems.

4. Challenges and Limitations in Federated Learning Adoption:

Despite its transformative potential, the widespread adoption of Federated Learning in digital banking faces **technical, operational, and organizational barriers**. One of the most significant challenges lies in **data heterogeneity**, where different banks or branches generate data with distinct distributions, features, and quality levels [13]. Such discrepancies can lead to model bias and slow convergence during global aggregation. Similarly, the need for frequent communication between clients and servers introduces **network latency** and synchronization issues, particularly in geographically dispersed systems.

Federated models also impose **high computational and storage demands** on local devices, especially when deep learning architectures are employed. This can strain resources in smaller financial institutions lacking advanced infrastructure [14]. Furthermore, the **interpretability of FL models** remains limited, complicating regulatory audits that require transparent explanations of automated decisions.

From a compliance perspective, integrating FL systems into existing cybersecurity infrastructures demands alignment with **industry standards and governance frameworks**. Banks must ensure that federated architectures adhere to security, auditing, and data management requirements mandated by financial authorities. Research suggests that adopting **robust aggregation protocols**, such as FedProx or adaptive federated averaging, can mitigate the impact of non-identically distributed data [15]. Likewise, hybrid FL architectures that combine **centralized and decentralized training elements** can balance efficiency and accuracy in large-scale deployments [16].

Operationally, organizations must address challenges such as **staff training**, **distributed resource management**, and **continuous model monitoring**. Developing skilled personnel capable of maintaining FL pipelines and interpreting federated outputs is essential for sustainable adoption [17]. Furthermore, consistent model validation is required to detect concept drift or adversarial manipulations that may compromise security.

Literature gap

Existing literature demonstrates the potential of Federated Learning for cybersecurity but lacks comprehensive studies focused specifically on digital banking systems. Most studies either address generic cybersecurity or financial fraud detection without integrating privacy-preserving FL frameworks. Additionally, empirical evidence on model performance in heterogeneous banking environments is limited. Few studies explore real-time deployment, scalability, and regulatory compliance simultaneously. This gap indicates the need for focused research examining FL implementation strategies, model optimization, and operational

challenges within the banking sector. Understanding these gaps will guide future research in designing effective, secure, and compliant FL-based cyber threat detection systems.

III. METHODOLOGY

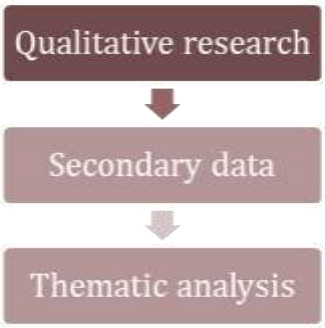

Fig 4: Methodology

This research adopts a secondary qualitative data analysis approach to investigate the application of Federated Learning for cyber threat detection in digital banking systems. Secondary qualitative research involves the systematic review and synthesis of existing scholarly literature, reports, and case studies [18]. This method allows the identification of trends, evaluation of methodologies, and discovery of gaps in current research without the need for primary data collection, which is sensitive in financial contexts.

The methodology involves a structured literature review. Initially, keywords such as "federated learning," "cybersecurity," "digital banking," and "intrusion detection" are identified and refined using Boolean operators. Academic databases, including IEEE Xplore, Scopus, and Web of Science, are utilized for comprehensive searches. Inclusion criteria focus on peer-reviewed articles published between 2020 and 2025, emphasizing practical applications, conceptual frameworks, and case studies of FL in cybersecurity. Exclusion criteria remove duplicates, irrelevant studies, or papers lacking sufficient methodological details [19].

Following the search, articles undergo critical appraisal for quality, relevance, and contribution to the research objectives. Selected studies are categorized based on their focus: FL applications, cyber threat detection techniques, privacy-preserving mechanisms, and deployment challenges [20]. Data extraction involves summarizing key findings, methodologies, results, and recommendations, which are then synthesized to identify patterns and insights relevant to banking systems.

The study applies thematic analysis to identify recurring themes in the literature [21]. Themes correspond to the objectives of the research, providing structured insights into FL adoption, benefits, challenges, and implementation strategies. This approach ensures rigorous analysis while maintaining focus on practical applicability. Findings are triangulated across multiple studies to enhance reliability and validity.

Ethical considerations in secondary data analysis are addressed by using publicly available, peer-reviewed sources, avoiding confidential banking data. This methodology provides a comprehensive understanding of the current state of FL for cyber threat detection, informing recommendations for future research and practical deployment in digital banking environments.

IV. DATA ANALYSIS

Theme 1: Applications of Federated Learning in Cybersecurity

Federated Learning (FL) has emerged as a transformative paradigm in **cybersecurity applications**, particularly within the financial services and digital banking sectors. Its fundamental advantage lies in enabling **collaborative model training** across distributed banking nodes without the need to centralize sensitive data. This decentralized approach allows financial institutions to build powerful, privacy-preserving machine learning models while ensuring compliance with stringent data protection regulations. According to recent studies, FL has demonstrated significant potential in **malware detection, phishing identification, and fraud prevention**, as well as in anomaly detection within financial transactions [22].

By distributing the learning process across multiple data silos such as different bank branches or affiliated institutions FL leverages

diverse datasets, thus enhancing the generalization and robustness of threat detection models. Traditional centralized systems require aggregation of raw data into a single repository, posing risks related to **data breaches, insider threats, and regulatory violations** [23]. FL mitigates these risks by sharing only model parameters or gradients rather than the underlying data, thereby protecting the confidentiality of customer information and transaction records.

Studies have applied a variety of federated model architectures, including **Federated Neural Networks (FNNs)**, **Federated Random Forests (FRFs)**, and **Federated Support Vector Machines (FSVMs)**, to detect emerging cyber threats. These models are capable of identifying subtle anomalies that may indicate coordinated attacks, distributed denial-of-service (DDoS) events, or fraudulent transactions. Comparative analyses have revealed that FL-based systems can achieve **accuracy levels comparable to centralized models**, while offering the additional benefits of privacy preservation and regulatory alignment [24].

Moreover, FL enables **cross-institutional collaboration** by facilitating secure knowledge sharing among banks. This collaboration enhances the collective intelligence of the sector, allowing institutions to respond more effectively to **system-wide vulnerabilities** that might otherwise go undetected if each organization operated in isolation. For example, an FL-based intrusion detection system (IDS) deployed across multiple financial entities can collectively recognize attack signatures that evolve or migrate between networks [25]. Such a system improves resilience and response time against **zero-day threats** and polymorphic malware.

Case studies demonstrate the integration of FL into **intrusion detection frameworks, fraud monitoring systems, and transaction validation platforms**. For instance, banks have deployed FL models that detect suspicious transaction patterns across geographically distributed nodes without transferring sensitive account data to a central location. However, operationalization challenges persist, particularly in synchronizing models across nodes with varying computational resources and network conditions [26]. **Data heterogeneity**—where different institutions maintain diverse data formats, volumes, and labeling standards—can impede model convergence and lead to inconsistent performance.

To address these challenges, the literature emphasizes the need for **adaptive aggregation protocols**, such as Federated Averaging (FedAvg) and its variants, which dynamically adjust weight updates to account for heterogeneous data [27]. Additionally, **communication-efficient strategies**, including model compression, asynchronous updates, and edge caching, have been proposed to reduce bandwidth overhead. Overall, Federated Learning presents a **scalable and privacy-preserving framework** for proactive cybersecurity in digital banking, enabling institutions to achieve stronger, data-driven defenses without sacrificing confidentiality or regulatory compliance [28].

Theme 2: Benefits and Limitations of Federated Learning in Digital Banking

The benefits of Federated Learning for digital banking include enhanced privacy, compliance with regulations, and improved collaborative threat intelligence. FL mitigates risks associated with centralized data storage and enables institutions to detect cross-organizational attack patterns. Literature identifies performance improvements in detecting zero-day attacks and evolving threats due to diverse data contributions [29]. Limitations include computational overhead, communication latency, and the complexity of managing heterogeneous datasets. Studies highlight issues such as uneven model performance across nodes, vulnerability to poisoning attacks, and challenges in integrating FL with legacy systems. Additionally, interpretability of FL models remains a concern, affecting regulatory transparency and stakeholder trust. Despite

these limitations, research suggests that hybrid approaches combining FL with local anomaly detection models can enhance performance while preserving privacy [30]. Optimization strategies, including adaptive learning rates and secure aggregation, are recommended to address technical barriers. The literature consistently emphasizes that the benefits of FL outweigh challenges, particularly when privacy and compliance are prioritized in banking operations.

Theme 3: Implementation Strategies and Operational Challenges

Effective implementation of FL in digital banking requires a comprehensive strategy addressing technical, operational, and regulatory dimensions. Literature identifies best practices, including establishing secure communication protocols, designing adaptive aggregation techniques, and ensuring model convergence under heterogeneous data conditions [31]. Operational challenges involve coordinating multiple banking nodes, training personnel, and integrating FL into existing cybersecurity frameworks. Studies also highlight the importance of monitoring model performance, handling data imbalance, and ensuring low-latency responses for real-time threat detection. Compliance with regulations such as GDPR and PCI DSS is crucial, requiring privacy-preserving techniques like differential privacy and homomorphic encryption [32]. Literature suggests phased deployment approaches, starting with pilot programs in limited branches, followed by gradual scaling across the institution. Collaboration among financial institutions can further enhance detection capabilities, but governance and trust mechanisms are essential to ensure data integrity. Overall, literature indicates that careful planning, infrastructure investment, and ongoing monitoring are critical for successful FL implementation in digital banking.

V. RESULTS AND DISCUSSION

The literature analysis demonstrates that Federated Learning presents a transformative approach for cyber threat detection in digital banking systems. Studies consistently reveal that FL allows collaborative model training across distributed banking nodes while maintaining privacy, addressing a critical limitation of traditional centralized cybersecurity systems [33]. Applications include malware detection, phishing identification, transaction anomaly detection, and fraud prevention. Models such as Federated Neural Networks, Random Forests, and ensemble approaches achieve detection rates comparable to centralized methods while preserving data confidentiality.

The analysis identifies several benefits of FL adoption. Privacy preservation is the primary advantage, ensuring regulatory compliance and mitigating risks of data breaches. Collaborative learning enables banks to leverage diverse data sources, enhancing detection of zero-day attacks and emerging threats [34]. Operational resilience is improved, as the distributed architecture avoids single points of failure, enabling continuous monitoring and response. Literature also highlights the flexibility of FL frameworks, which can integrate with existing intrusion detection systems, fraud monitoring platforms, and transaction analysis tools.

However, the studies reveal significant challenges and limitations. Heterogeneous data across banking nodes can lead to uneven model performance, requiring adaptive aggregation and weighting strategies [35]. Communication latency and computational overhead can impede real-time detection, emphasizing the need for optimized model architectures. Security concerns, including poisoning attacks and model inversion, must be addressed through robust privacy-preserving mechanisms [36]. Operational adoption involves training personnel, coordinating distributed nodes, and integrating FL into legacy banking systems. Additionally, model interpretability is critical for regulatory compliance, necessitating explainable AI techniques.

The literature underscores the importance of implementation strategies. Pilot deployments, phased scaling, and cross-institution collaboration are recommended to mitigate technical and operational risks. Privacy-preserving methods, such as differential privacy and homomorphic encryption, are essential for secure deployment. Studies emphasize ongoing monitoring and evaluation to maintain model performance, adapt to evolving cyber threats, and ensure compliance. The literature confirms that Federated Learning holds substantial promise for enhancing cybersecurity in digital banking. Its ability to balance privacy, collaborative intelligence, and operational resilience addresses major gaps in traditional threat detection methods. While challenges exist, research suggests that careful design, robust privacy mechanisms, and adaptive strategies enable effective deployment. The findings indicate that FL can transform cyber threat detection, providing secure, efficient, and scalable solutions for modern banking systems.

Limitations

Despite its potential, Federated Learning (FL) faces several limitations in digital banking cybersecurity. Heterogeneous data across different banking branches or institutions can result in uneven model performance, reducing overall detection accuracy [27]. Communication overhead between distributed nodes can introduce latency, affecting real-time threat detection. FL models are also susceptible to security threats, including model poisoning and adversarial attacks, which may compromise reliability. Computational complexity and high resource requirements pose challenges for banks with limited infrastructure. Additionally, the interpretability of FL models is limited, complicating compliance with regulatory frameworks such as GDPR and PCI DSS. Integration with legacy systems and ensuring seamless operation alongside existing security mechanisms also remain significant challenges, requiring careful planning and technical expertise.

Implementation

Effective implementation of Federated Learning in digital banking requires a structured, multi-phase approach. Initially, pilot programs should be conducted in select branches to evaluate performance, latency, and model accuracy under real-world conditions. Secure communication protocols, encryption, and privacy-preserving techniques like differential privacy should be integrated to protect sensitive data. Adaptive aggregation strategies can address data heterogeneity and improve convergence across distributed nodes. Training personnel, establishing cross-institution governance frameworks, and monitoring model performance are essential for operational success. Integration with existing intrusion detection systems, transaction monitoring platforms, and fraud detection frameworks ensures comprehensive cybersecurity coverage. Continuous evaluation, model updates, and scalability planning allow FL to remain effective against evolving cyber threats while maintaining regulatory compliance and operational efficiency.

VI. FUTURE STUDY

Future research should focus on empirical evaluation of Federated Learning in operational banking environments, examining real-world performance, latency, and scalability. Studies could explore hybrid approaches combining FL with local anomaly detection models to enhance performance and resilience against sophisticated attacks. Research on adaptive aggregation strategies for heterogeneous banking datasets is necessary to address model convergence challenges. Privacy-preserving mechanisms should be optimized to balance security, computational efficiency, and regulatory compliance. Additionally, future studies could investigate integration of explainable AI techniques within FL models to improve interpretability for stakeholders and regulators [38]. Cross-institution collaborations can be

analyzed to develop governance frameworks for secure data sharing and collaborative threat intelligence. Exploring the economic and operational implications of FL adoption, including cost-benefit analyses and infrastructure requirements, will further support informed decision-making by financial institutions seeking to implement advanced cybersecurity strategies.

VII. CONCLUSION

The research demonstrates that Federated Learning offers a practical, privacy-preserving approach to cyber threat detection in digital banking systems. Literature analysis confirms that FL enables collaborative model training across distributed nodes, improving detection of malware, phishing attacks, and transaction anomalies while maintaining regulatory compliance. Key benefits include enhanced data privacy, operational resilience, and improved threat intelligence through shared learning across institutions. Limitations such as communication latency, heterogeneous data, computational overhead, and model interpretability require careful management. Implementation strategies involving secure aggregation, privacy-preserving mechanisms, phased deployment, and cross-institution collaboration are critical for success. The study identifies gaps in empirical evidence, real-time deployment strategies, and regulatory integration, indicating areas for future research. Overall, FL presents a scalable, effective, and secure framework for digital banking cybersecurity, addressing the shortcomings of traditional centralized systems while enabling collaborative, intelligent, and privacy-compliant threat detection.

VIII. REFERENCE

[1] Gajula, S. (2025). Cybersecurity in Supply Chain Management: Role of Identity and Access Management, Zero Trust, and Blockchain. *Asian Journal of Computer Science Engineering (AJCSE)*, 10(2), pp.1–11.

[2] Paruchuri, V.B. (2021). Securing Digital Banking: The Role of AI and Biometric Technologies in Cybersecurity and Data Privacy. *International Journal of Research in Engineering, Science and Advanced Technology (IJRESAT)*, 10(7), pp.128–133. ISSN 2456–5083.

[3] Haque, A.B., Islam, A.N., Hyrynsalmi, S., Naqvi, B. and Smolander, K., (2021). GDPR compliant blockchains–a systematic literature review. *Ieee Access*, 9, pp.50593-50606.

[4] Kovvuri, V.K.R. (2025). AI-Driven Cybersecurity Solutions for Cloud-Native Applications: Challenges and Future Directions. *SSRN Electronic Journal*, Paper No. 5283693.

[5] Todupunuri, A. (2023). The Role of Artificial Intelligence in Enhancing Cybersecurity Measures in Online Banking Using AI. *International Journal of Enhanced Research in Management & Computer Applications*, 12(1), pp.103–108.

[6] Banda, S. (2025). AI-based transaction risk scoring framework for credit card platforms: A TSYS-compatible architecture in Java. *SSRN Electronic Journal*, Paper No. 5331134.

[7] Kotte, G. (2025). Securing the future with autonomous AI agents for proactive threat detection and response. *International Research Journal of Economics and Management Studies (IRJEMS)*, 4(5), pp.165–170.

[8] Todupunuri, A. (2024). Explore How AI Can Be Used to Create Dynamic and Adaptive Fraud Rules That Improve the Detection and Prevention of Fraudulent Activities in Digital Banking. *International Journal of Research and Analytical Reviews (IJRAR)*, 13(9), pp.372–377.

[9] Duvvuri, J.R. (2024). Integrating Camunda and Activiti and the Role of React in Innovating Banking Systems. *Journal of Scientific and Engineering Research*, 11(4), pp.380–386.

[10] Darreddy, J.K.R. (2025). Revolutionizing ServiceNow GRC with Generative AI: The Future of AI-Driven Governance. *International Journal of Applied Science, Engineering and Management (IJASEM)*, 19(1), pp.586–590.

[11] Banda, S. (2025). Exploring data-driven innovation through cloud-native architectures in enterprise systems.*SSRN Electronic Journal*, Paper No. 5283830.

[12] Kanagarla, K.P.B. (2024).Explainable AI in Data Analytics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, 10(3), pp.56–62.

[13] Kumar, J.K.R. (2024). Enhancing Customer Experience Using AI-Based Recommendation Systems in E-Commerce. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(4), pp.83–88.

[14] Kanagarla, K.P.B. (2024). The Role of Synthetic Data in Ensuring Data Privacy and Enabling Secure Analytics. *European Journal of Advances in Engineering and Technology (EJAET)*, 11(10), pp.75–79.

[15] Munagala, M.K. (2025). Integrating AI and DevOps Practices to Develop Cybersecurity Frameworks that Enhance Resilience in Utility Infrastructure. *Journal of Informatics Education and Research (JIER)*, 5(2), pp.3646–3650. ISSN 1526-4726.

[16] Alazab, M., Rm, S.P., Maddikunta, P.K.R., Gadekallu, T.R. and Pham, Q.V., (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics*, 18(5), pp.3501-3509.

[17] Varga, S., Brynielsson, J. and Franke, U., (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, 105, p.102239.

[18] Kanamori, S., Abe, T., Ito, T., Emura, K., Wang, L., Yamamoto, S., Phong, L.T., Abe, K., Kim, S., Nojima, R. and Ozawa, S., (2022). Privacy-preserving federated learning for detecting fraudulent financial transactions in japanese banks. *Journal of Information Processing*, 30, pp.789-795.

[19] Rongali, L.P. (2025). Data Mesh: Decentralised Data Management. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 14(3), pp. 45–50.

[20] Paruchuri, V.B. (2023). AI-Enhanced Business Intelligence Framework for Predictive Financial Analytics. *Journal of Accounting, Auditing and Finance Research (JAAFR)*, 3(7), pp.1–9. ISSN 2788–718X.

[21] Prodduturi, S.M.K. (2024). Investigating the Challenges and Opportunities of Cybersecurity in the Era of Remote Work. *European Journal of Advances in Engineering and Technology (EJAET)*, 11(10), pp.80–84. ISSN 2394-658X.

[22] Awosika, T., Shukla, R.M. and Pranggono, B., (2024). Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection. *IEEE access*, 12, pp.64551-64560.

[23] Bakare[1], S.S., Adeniyi, A.O., Akpuokwe, C.U. and Eneh[4], N.E., (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations.

[24] Kovvuri, V.K.R. (2025). AI-Powered Customer Engagement Frameworks for Financial Services. *SSRN Electronic Journal*, Paper No. 5238422

[25] Ghelani, D., Hua, T.K. and Koduru, S.K.R., (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints.*

[26] Rongali, L.P. & Budda, G.A.K. (2025). Integrating AI and DevOps Practices to Develop Cybersecurity Frameworks that Enhance Resilience in Utility Infrastructure. *Journal of Informatics Education and Research (JIER)*, 5(2), pp. 10–15

[27] Prodduturi, S.M.K. (2025). AI-Enhanced Mobile Application Development: Leveraging Machine Learning for Real-Time User Interaction. *International Journal of Modern Engineering and Technology (IJMET)*, 15(2), pp.145–150.

[28] Sarhan, M., Layeghy, S., Moustafa, N. and Portmann, M., (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, 31(1), p.3.

[29] Kumar, J.K.R. (2024). Leveraging Predictive Analytics for Supply Chain

Optimization in Manufacturing. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 15(6), pp.110–115.
[30] Hassan, W. and Mohamed, H., (2024). Applications of federated learning in AI, IoT,
[31] babu Nuthalapati, S., (2023). AI-enhanced detection and mitigation of cybersecurity threats in digital banking. Educ. Adm. *Theory Pract.*, 29(1), pp.357-368.
[32] Das, S.S. (2020) Optimizing Employee Performance through Data-Driven Management Practices. *European Journal of Advances in Engineering and Technology (EJAET)*, 7(1), pp.76–81.
[33] Oyewole, A.T., Okoye, C.C., Ofodile, O.C. and Ugochukwu, C.E., (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), pp.625-643.
[34] Islam, U., Muhammad, A., Mansoor, R., Hossain, M.S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U. and Shafiq, M., (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability*, 14(14), p.8374.
[35] Das, S.S. (2025) Intelligent Data Quality Framework Powered by AI for Reliable, Informed Business Decisions. *Journal of Informatics Education and Research*, 5(2), pp.4748–4754.
[36] Wang, S., Asif, M., Shahzad, M.F. and Ashfaq, M., (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & security, 147, p.104051.
[37] Kumar, V. and Sinha, D., (2021). A robust intelligent zero-day cyber-attack detection technique. *Complex & Intelligent Systems*, 7(5), pp.2211-2234.
[38] Kotte, G. (2023). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. *SSRN Electronic Journal*, Paper No. 5283668.
healthcare, finance, banking, and cross-domain learning. *In Artificial Intelligence Using Federated Learnin*g (pp. 175-195). CRC Press.