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

(Review Article)

Federated learning in University IT security: A conceptual framework for privacy-preserving cyber threat detection

Ifeoluwa Uchechukwu Wada [1, *], Gideon Olawale Sodipo [2], Temitope Babayemi [3], Abdullahi Abdulkareem [4] and Aghoghomena Emadoye [5]

[1] Information Technology Services, Washburn University, Topeka, KS USA.
[2] Department of Computer Science, Kent State University, Kent, Ohio USA.
[3] School of Business and Technology, Emporia State University, KS, USA.
[4] College of Business, Lamar University, Texas, USA.
[5] Department of Finance, 10Alytics Inc, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 2236-2244

Publication history: Received on 05 March 2025; revised on 14 April 2025; accepted on 16 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1309

Abstract

As the alarming rate of cyber threats increases in higher education institutions, the challenge of protecting sensitive data while ensuring efficient threat detection becomes more complex. There is a risk of violating data privacy standards such as Family Educational Rights and Privacy Act (FERPA) and General Data Protection Regulation (GDPR) while using traditional cybersecurity methods. Federated Learning (FL) mitigates this by allowing decentralized model training without sharing raw data. This paper proposes a novel conceptual framework for applying FL in university IT security systems. By allowing departments to train local threat detection models without sharing raw data, the framework preserves confidentiality while enabling collaborative learning across institutional silos. This research employs a design science approach outlining the framework's architecture, key components, privacy-enhancing techniques, and implementation considerations. It also explores the potential benefits such as improved detection accuracy, and regulatory compliance as well as limitations related to system heterogeneity and communication overhead. The study concludes by identifying future directions for pilot implementation. This work contributes to a scalable, adaptable solution for strengthening cybersecurity across the higher education landscape while upholding institutional autonomy and privacy.

Keywords: Federated Learning; Cybersecurity; Artificial Intelligence; Higher Education Institutions; Data privacy

1. Introduction

Universities and colleges globally are experiencing a surge in cybersecurity attacks, ranging from phishing schemes to ransomware attacks targeting sensitive students, faculty, and institutional data. Unlike corporate IT systems, university infrastructures are mainly decentralized, comprising of different departments, user groups, campuses, and systems with different security policies. This heterogeneity, coupled with the need to comply with strict data privacy laws such as FERPA and GDPR, makes centralized cybersecurity solutions very tough. This decentralized structure has gained a lot of attention recently[1]. Some common cyber-attacks in universities include phishing, data breaches, ransomware and unauthorized access to data[2].

Traditional cybersecurity mechanisms often depend on centralized data collection and analysis to detect and mitigate cyberattacks. These systems could bring about data privacy challenges in the education sector. Centralizing data from different departments could raise ethical issues surrounding data sharing under strict privacy regulations such as

[*] Corresponding author: Ifeoluwa Uchechukwu Wada

FERPA and GDPR. Recently, machine learning has been increasingly used and proven effective in detecting cyberthreats[3]. Federated Learning (FL), a machine learning approach that enables model training across decentralized devices or servers without transferring raw data[4], offers a compelling solution to this challenge by providing a method for preserving privacy while detecting cyberattacks[5]. FL has demonstrated success in privacy-sensitive sectors like healthcare and fintech, where data privacy is key. However, research on the application of FL in university IT security is still in its infant stage. This paper aims to bridge this research gap by proposing a conceptual framework for deploying FL in higher education cybersecurity systems to enhance threat detection while preserving institutional and user privacy. This research aims to contribute to the unique operational and ethical challenges of higher education institutions (HEIs).

The key research questions guiding this study are:

- RQ1: How can Federated Learning be effectively used to detect cyber-attacks within a University's IT infrastructure?
- RQ2: What design requirements are needed for a privacy-preserving federated cybersecurity framework tailored to HEIs?
- RQ3: What are the benefits, challenges and limitations of adopting Federated learning for threat detection in HEIs?

2. Literature Review

2.1. Cybersecurity Landscape in Higher Education

There has been an increase in cyber threats in HEIs [6]because of their open access network and decentralized structure. Different academic users from faculty, staff, students and third-party vendors and researchers need different levels of access to resources in academia. This poses a unique security challenge to the academic's landscape. A vast amount of data including Personally Identifiable Information (PIIs) are stored in HEIs making them major targets for cyberattacks[6].

Data privacy is a major concern in the education section thus many institutions hold back in sharing students' data raising the need for cybersecurity methods without direct exchange of data[7]. Federated learning (FL) has provided an effective approach that allows for distributed machine learning in compacting cyberthreats without compromising data security and privacy[3]. In similar sectors that require high levels of data security, FL has been utilized to train models that can detect cyberattacks and mitigate them. In healthcare, FL has been used to train models on patient data stored across different hospitals. In 2020, a brain tumor segmentation model was developed using FL across multiple institutions[8]. The FL approach allowed for collaboration without the need to share patient data, thus complying with The Health Insurance Portability and Accountability Act (HIPAA) regulations.

2.2. Limitations of Traditional Cybersecurity Methods in HEIs

In HEIs, traditional cybersecurity systems usually depend on centralized architectures where logs, network traffic and user activity are collected[9]. This approach has been working over the years however with the increasing AI-enabled cyber threats, several limitations have arisen with this traditional cybersecurity method. Privacy risks have been a major concern over the years. Aggregating sensitive data from different departments can bring about the violation of data regulations such as FERPA and GDPR. A single point of failure is another major concern as a breach of the central system can compromise all data collected, making it a lucrative target for cyberattacks[10]. These limitations call for the need for a decentralized, privacy- preserving cybersecurity method in the academic landscape.

2.3. Federated Learning

In traditional machine learning, there is a transfer of data from different points or devices to the centralized cloud to train the model [11]. In this process, there is a risk of exposing sensitive data like student data, research data, individual location data and research data to potential attackers. There is an urgent need for innovative technologies for achieving data privacy and mitigating these cyber threats[12]. Thus, the need for Federated Learning. Federated Learning works by training a machine learning model without sharing raw data to external sources [13]. FL works by protecting the privacy of users by exchanging parameters that have been encrypted while cyber attackers are unable to get the data source [14] . Thus, there is no risk of leaking privacy at the data level and no risk of violating data compliance laws. FL serves as a solution to data security and privacy issues during data collection[15]. One major characteristic of FL is that it ensures a decentralized environment for the data available [16]. This also ensures that the machine learning model can learn via aggregation. A study by [17] showed FL's efficacy through its privacy- preserving methods, decentralized model updates and safe methods of data aggregation. Key features of FL include its data locality, collaborative learning and enhanced security. These reduce the dangers associated with centralized repositories [18]. Banks and financial institutions have used FL for fraud detection and anti-money laundering by collaboratively training models across different organizations without exposing sensitive data. This ensures compliance with data protection laws while improving model accuracy and robustness.

2.4. Applications of Federated Learning in Cybersecurity

Although FL is relatively new, it is being increasingly explored in different sectors where data privacy is extremely important, like education, healthcare and finance. Governmental agencies are exploring FL to enable secure collaboration between jurisdictions for various activities like threat detection and intelligence sharing. These implementations prioritize data sovereignty and privacy compliance. These applications confirm FL's ability to operate in highly sensitive and regulated environments, making it a strong candidate for use in higher education cybersecurity.

In 2022, a novel Federated Deep Learning Intrusion Detection System (IDS) was developed to detect cyber-attacks in smart Internet of Things (IoT) systems using Generative Adversarial Network (GAN)[19]. The system provided a more secure solution for the detection of intrusion in smart environments. In 2024, an adaptive Federated Learning approach to DDoS attack detection (FLAD) was proposed[20] . This model did not require the sharing of test data and was effective in identifying cyber threats. As demonstrated by [21], a Privacy-preserving Federated Learning (PPFL) framework can significantly improve data privacy and detect cyber threats. CYBRIA, another federated learning framework proposed by[22] was effective in preserving data while combating cyber threats. This framework trained models on separate local data distributed amongst clients and shared only intermediate updates from the model to generate an integrated global model.

2.5. Privacy Regulations and FL Suitability

2.5.1. Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act protects student education records in the United States. FERPA limits the sharing of personally identifiable information within and outside the institution[23]. FL ensures that sensitive educational data never leaves departmental servers.

2.5.2. General Data Protection Regulation (GDPR)

The General Data Protection Regulation applies to institutions handling data of individuals within the European Union[24]. This regulation places strict rules on consent, data minimization, and data localization. FL supports GDPR compliance by ensuring decentralized data processing and offering mechanisms for user consent and auditability.

2.5.3. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA aims to ensure the privacy and security of medical records and other personal health information [25]. Universities with medical centers or health programs must comply with HIPAA regulations. FL has been used in healthcare to ensure privacy and compliance with HIPAA regulations by training diagnostic models without the sharing of sensitive patient data.[26].

By addressing the core tenets of these regulations, FL presents itself as a privacy-first architecture for cybersecurity in educational institutions.

3. Methodology

This research adopts a conceptual research design aimed at developing a novel FL framework for cyber threat detection in University IT environments. The research follows a design science approach, rooted in existing literature, practical constraints in the academia landscape and principles from federated learning and Artificial Intelligence domains.

3.1. Research Design Approach

The methodology involves four major stages:

- Literature Review: The study begins with a comprehensive review of scholarly and technical literature including peer reviewed journal articles on federated learning, privacy preserving machine learning and cybersecurity in educational and other data sensitive institutions as well as regulatory frameworks such as FERPA, GDPR and institutional privacy mandates. This review includes identifying research gaps, limitations and opportunities in existing studies. It also evaluates the suitability of FL as a solution for decentralized privacy-sensitive environments.

- Problem Contextualization: This involves mapping unique cybersecurity challenges faced by HEIs such as data decentralization, privacy concerns and regulatory compliance to federated methodology requirements. Based on the insights from the literature, the study identifies major requirements for an effective cybersecurity framework in University IT settings. These requirements include preserving data privacy, accommodating the decentralized academics landscape, enabling the detection and mitigation of cyber threats and ensuring compliance with regulatory bodies.
- Conceptual Framework Development: This synthesizes the insights and specified requirements into a conceptual framework tailored for the academic industry. This includes data flows, components, mechanisms and strategies for integration. The roles and responsibilities of the local nodes such as academic departments were outlines as well as the functionality of a central aggregation server. This conceptual framework is informed by best practices in FL as well as threat models and the different operational workflows in the HEIs landscape.
- Validation through theoretical alignment: This evaluates the proposed framework against the principles of distributed learning, privacy preserving models and higher education cybersecurity policies like FERPA and GDPR. Although no experimental validation is carried out, strong emphasis is made on theoretical consistency and applicability.

3.2. Rationale for Conceptual Approach

As a result of the infant stage of applying FL in university cybersecurity, a conceptual framework provides a strong foundation for future research and implementation. This approach enables a clear understanding of how FL can address the unique academia landscape. It also allows flexibility to adapt the model to different institutional contexts. This framework allows future empirical studies to test and refine it. By building a clearly defined and structured model, this paper provides a solution that is privacy conscious and scalable and can inform practical deployment in higher education cybersecurity.

4. Conceptual Framework: FL for University Cybersecurity

4.1. Framework Overview

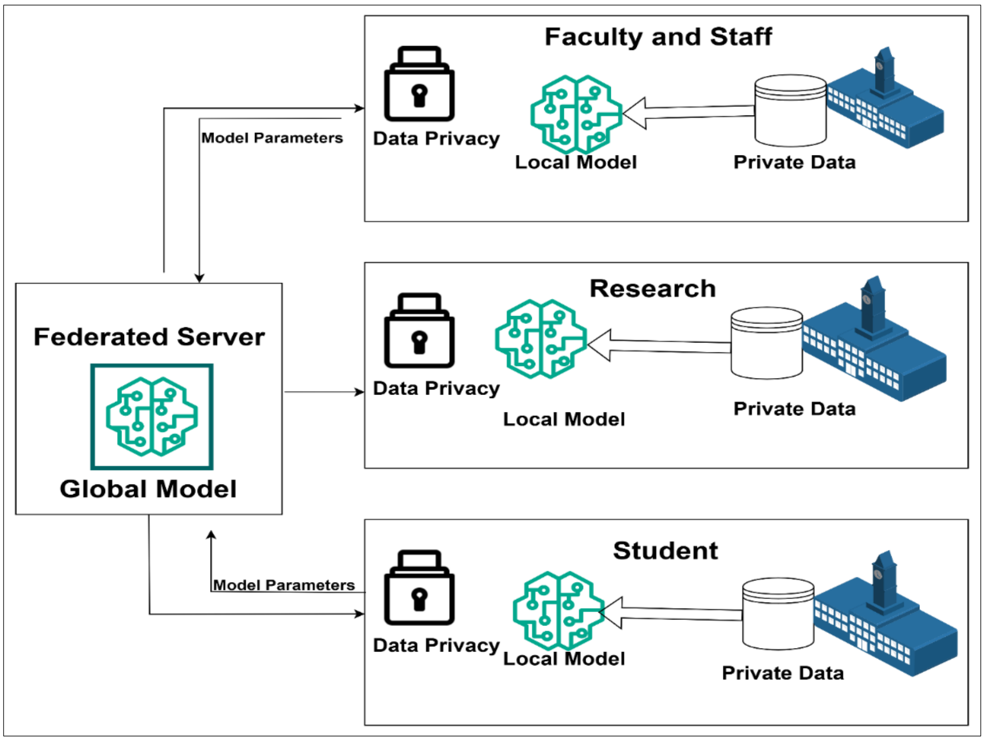

Figure 1 A conceptual framework for privacy-preserving cyber-threat detection in Higher Education Institutions

The proposed FL- based cybersecurity framework allows for different departments and units within a university to train a machine learning model collaboratively without sharing raw data. In this framework, the individual departments retain their data locally, for example, each department retains its system events, access requests and user activity logs, and trains a local model for detecting threats. Only model updates are sent to a central server which then aggregates to form a global mode (Fig 1). This process will ensure data privacy by ensuring that sensitive data never leaves the originating department. This framework is highly adaptive and iterative, ensuring that departments can continually contribute to and benefit from an improved threat detection system without the compromise of data integrity or violation of data privacy regulations.

4.2. Key Components

The proposed framework is composed of three major primary components, each of which plays a distinct role in enabling decentralized, privacy- preserving cyber-attack detection in the academic community.

- Local Learning Clients (LLCs): These consist of different computing entities located in different departments, faculties or administrative units of the university for example campus servers, department-level systems and IoT devices. Each LLC is responsible for the collection and secure storage of local cybersecurity data such as user access logs and network traffic patterns. LLCs also preprocess data to remove sensitive information, trains a local threat detection using machine learning algorithms and transmits only model parameters and not raw data to the aggregation server.
- Central Aggregation Server (CAS): This includes University-wide or consortium-level servers that are used to aggregate the models. The central node receives model updates from all the Local Data Nodes (LDNs) and carry out secure aggregation like federating averaging. The server updates the global model and shares the updated model with all the LDNs. It also includes privacy-enhancing techniques such as homomorphic encryption.
- Federated Learning Controller (FLC): This is a management layer that performs the coordination of training rounds, monitoring of model convergence as well as managing participation and trust among the different nodes. In this layer, privacy is enforced.

4.3. Privacy Preservation Strategies

This framework integrates various privacy preservation methods to ensure that the FL procedures align with ethical and legal standards. These include differential privacy, secure aggregation and anonymization. In differential privacy, statistical noise is added to the model to prevent reverse engineering of the original data. Secure Aggregation makes use of cryptographic procedures to ensure that the central aggregation server cannot view individual updates, rather it only accesses the combined result. Data minimization and anonymization preprocesses the log data to strip personally Identifiable Information before training the local models. These techniques ensure compliance with policies such as FERPA, GDPR and institutional data policies.

4.4. Model Training and Workflow

The FL model is trained to recognize and mitigate cyber threats such as insider misuse, brute-force login attempts and privilege escalation. Each LDN may encounter unique patterns because of contextual differences which enrich the global model. The iterative training of the model ensures the detection of common and context specific attackers, enhanced generalization of threats and faster response time to emerging threats without the need for centralized retraining

The workflow is designed to be modular, scalable and flexible. Each campus node trains a model locally on its security data. The model updates only and not raw data are encrypted and sent to the aggregator after which the aggregator combines updates into a global model (fig 2). The updated global model is sent back to nodes for further training, and this is repeated until convergence. The data sources for local training include network logs, user authentication data, endpoint detection system, email metadata (not content).

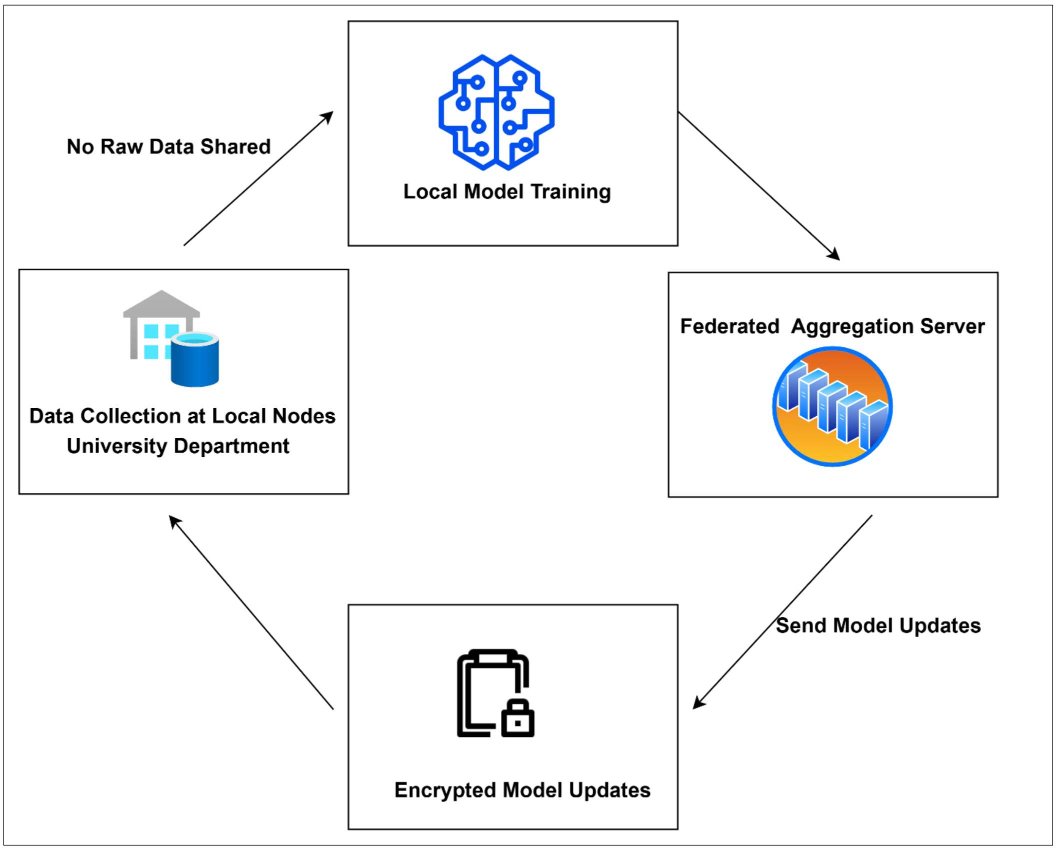
Local Model Training
No Raw Data Shared
Federated Aggregation Server
Data Collection at Local Nodes University Department
Send Model Updates
Encrypted Model Updates

Figure 2 Federated Learning Model Workflow for Cyber Threat Detection

5. Implementation Challenges and Considerations

The Implementation of the proposed framework in a university landscape requires careful attention to technical, organizational and policy related factors. Key practical considerations for successful deployment and operation are outlined in this session.

5.1. Data Sources and Types

In the university landscape, a wide range of data streams are generated by the IT systems which are suitable for threat detection. Depending on the operational structure, each department may produce unique data sets which require local data normalization before it can be used in the FL model training. Some common sources of data include network traffic (such as unusual data flow, port scanning activity), authentication logs (such as login attempts, and password resets) and access control logs (such as system privileges and file access patterns).

5.2. Platform Compatibility

To ensure seamless adoption across diverse departments, the FL framework must be compatible with the existing IT and cybersecurity tools such as log management platforms, SIEM systems and endpoint detection systems.

5.3. Communication and Network Requirements

FL involves frequent communication between local nodes and the aggregation server. Bandwidth optimization is important especially when many units or departments simultaneously participate. Compression techniques can be applied to reduce the size of the transmitted model updates. Latency can be reduced through asynchronous updates and encrypted channels such as Transport Layer Security (TLS) or Secure Socket Layers (SSL) must be enforced to ensure that the data in transit is secure during the exchange of model parameters.

5.3.1. Privacy and Security Enhancements

It is important to put measures in place to ensure compliance with data protection laws and institutional policies. Differential privacy mechanisms should be applied to local model updates before they are transmitted. It is also important to ensure secure aggregation by using secure multiparty computation (SMPC) or homomorphic encryption in sensitive environments. Access controls and audit trails must be in place to monitor the behavior of both local nodes and the aggregator. These security measures protect against model inversion attacks, gradient leakage, and malicious node manipulation.

5.3.2. Monitoring, Maintenance, and Model Updates

Continuous monitoring and evaluation are essential to ensure the continued performance of the model. Model drift detection should be employed to identify when threat patterns evolve, and retraining is necessary. It is important to track accuracy, false positive/negative rates, and department-level contributions using performance dashboards. Periodic updates to the global model must be scheduled with minimal disruption to local operations. Logging and audit capabilities are also critical for ensuring accountability and diagnosing issues.

6. Benefits and Limitation

The proposed Federated Learning framework offers an innovative approach to enhancing cybersecurity in university IT systems. By preserving data locality and decentralizing model training, it addresses the limitations of traditional cybersecurity which entails a centralized approach. However, the successful deployment of this model requires meticulous navigation of operational and technical challenges. The benefits and limitations of this framework are discussed in this section

6.1. Benefits

One key benefit of this model is privacy preservation because this framework is centered on the principle of data minimization. FL ensures that sensitive institutional data such as student records, faculty credentials, and research logs never leaves the originating departments. This significantly reduces exposure to privacy breaches and supports compliance with regulations such as FERPA (Family Educational Rights and Privacy Act), GDPR (General Data Protection Regulation) and Institutional data governance policies.

This framework also allows for collaborative learning across silos. It is often difficult to share threat intelligence because of the way universities function in departmental silos. The FL approach enables cross-departmental collaboration without the need for centralized data pooling, allowing the detection model to learn from a diverse and representative set of threats. A key advantage of this model is improved threat detection. Local models capture context-specific behaviors (e.g., research lab activity vs. student portals) thus, the global model becomes better at detecting a wider range of anomalies. This results in a higher detection accuracy, faster adaptation to emerging threats as well as a reduction in false positives and negatives. Another major benefit of this framework is that it reduces the single point of failure. Unlike centralized systems where a breach or outage can compromise the entire detection infrastructure, this framework distributes risk. Compromising one local node does not expose the entire system.

6.2. Limitations and Challenges

Just like all systems, this framework also has its limitations and challenges. A major limitation in the university landscape is system heterogeneity. Universities use a wide range of hardware, software, and security protocols across departments. Thus, this variation can complicate local data preprocessing and standardization or affect the model convergence and consistency. Communication overhead is another challenge that can limit the functionality of this framework. Frequent exchange of model updates, especially during training rounds can strain university networks and introduce latency. This requires bandwidth-efficient protocols and asynchronous update mechanisms. Another challenge that is worth noting is the limited computing resources at local nodes. Not all departments may have the technical capacity or computing infrastructure to train local models effectively. This creates imbalances in participation and may require resource provisioning or shared support. While FL enhances privacy, it introduces new security risks such as poisoning attacks, where compromised nodes send misleading model updates or gradient leakage, where attackers attempt to reconstruct sensitive data from model updates. To mitigate this, there must be robust validation protocols, anomaly detection, and secure aggregation in place. Cultural and administrative barriers possess another challenge to the successful implementation of this framework. Differences in awareness, expertise, and willingness to participate can hinder adoption unless backed by strong institutional leadership and policies.

7. Future Directions

This framework lays the foundation for a privacy -preserving federated approach to cyber threat detection in university IT systems. As there is an increase in the adoption of FL in cybersecurity, there are several promising avenues for the future exploration and practical deployment of this model. A pilot version of this framework can be implemented in a controlled environment to provide empirical insights into performance, deployment feasibility and organizational readiness. This would help identify bottlenecks related to model convergence, network latency or cross departmental coordination.

8. Conclusion

Federated Learning presents a transformative opportunity for higher education institutions to enhance cybersecurity without compromising privacy. As universities continue to digitize their academic, research and administrative operations, the need for a robust, privacy-preservation cybersecurity solution increases. By leveraging decentralized intelligence and preserving sensitive data at its source, universities can stay ahead of evolving cyber threats.

This paper proposes a conceptual framework for applying Federated Learning (FL) to cyber threat detection within university IT ecosystems. By enabling decentralized model training across departments while keeping sensitive data local, the framework offers a scalable and compliant solution that aligns with the operational structure of higher education. The proposed architecture leverages FL's strengths which include data locality, collaborative learning, and data privacy to enhance the institution's ability to detect and respond to cyber threats effectively. Through a structured methodology grounded in design science and informed by current literature, the framework addresses critical technical and policy-related concerns. It outlines core components, implementation considerations, and potential privacy-preserving strategies such as differential privacy and secure aggregation. Additionally, it anticipates real-world deployment challenges, including system heterogeneity, communication overhead, and organizational barriers, while also identifying future directions for pilot implementation.

In conclusion, Federated Learning represents a promising shift in how universities can secure their digital environments without compromising the privacy and autonomy of their departments. This framework serves as a foundation for future research, development, and institutional adoption, contributing to the evolution of innovative, ethical, and intelligent cybersecurity infrastructures in the education sector

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] B. Ghimire and D. B. Rawat: Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. IEEE Internet Things J. 2022;9(11): 2022.

[2] Suzzanne Nzingo Kalume and Dr. Shadrack Ochieng Owiti. Cybersecurity Challenges, Strategies and Emerging Trends in Higher Education Institutions-A Survey A Survey. EPRA International Journal of Research & Development (IJRD). 2025: 98–103.

[3] A. Alazab, A. Khraisat, S. Singh, and T. Jan. Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. Electronics (Basel). 2023; 12(16):3382.

[4] G. K. Jagarlamudi, A. Yazdinejad, R. M. Parizi, and S. Pouriyeh. Exploring privacy measurement in federated learning. J Supercomput. 2024; 80(6): 10511–10551.

[5] M. Ragab , E Bahaudien Ashary, B. Alghamdi, R. Aboalela, N. Alsaadi L Maghrabi, K.Allehaibi. Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. Scientific Report. 2025; 15(1): 4470.

[6] Ifeoluwa Uchechukwu Wada, Godwin Osezua Izibili, Temitope Babayemi, Abdullahi Abdulkareem, Oluwabukunmi M. Macaulay, and Aghoghomena Emadoye. AI-driven cybersecurity in higher education: A

systematic review and model evaluation for enhanced threat detection and incident response. World Journal of Advanced Research and Reviews. 2025; 25(3):89-90.

[7] S. Guo and D. Zeng. Pedagogical Data Federation toward Education 4.0. in ACM International Conference Proceeding Series. 2020.

[8] M. J. Sheller , Brandon Edwards, G Antony Reina, Jason Martin, Sarthak Pati, Aikaterini Kotrotsou, Mikhail Milchenko, Weilin Xu, Daniel Marcus, Rivka Colen, Spyridon Bakas. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Sci Rep. 2020; 10(1): 12598.

[9] E. C. K. Cheng and T. Wang. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (Switzerland). 2022; 13(4):90.

[10] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit. Privacy and Security in Federated Learning: A Survey. Applied Sciences (Switzerland). 2022; 12(19):33.

[11] M. Alazab, P. R. Swarna, Praveen Kumar Reddy Maddikunta, T. R. Gadekallu, and Q.-V. Pham. Federated learning for cybersecurity: Concepts, challenges, and future directions. IEEE Transactions on Industrial Informatics. 2021;18(5):501–3509.

[12] M. Aloqaily, S. Kanhere, P. Bellavista, and M. Nogueira. Special Issue on Cybersecurity Management in the Era of AI. Journal of Network and Systems Management. 2022;30(3): 29.

[13] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb. Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems. IEEE Communications Surveys and Tutorials. 2021; 23(2):1109.

[14] B. Yu, W. Mao, Y. Lv, C. Zhang, and Y. Xie. A survey on federated learning in data mining. 2022.

[15] J. C. Jiang, B. Kantarci, S. Oktug, and T. Soyata. Federated learning in smart city sensing: Challenges and opportunities. 2020.

[16] B. Dash, P. Sharma, and A. Ali. Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech. International Journal of Software Engineering & Applications. 2022;13(4):10.

[17] M. Ashok Kumar, A. Mohammed, S. Sumanth, and V. Sivanantham. Enhancing Cybersecurity Through Federated Learning: A Critical Evaluation of Strategies and Implications in Model Optimization Methods for Efficient and Edge AI. Wiley. 2025: 281-297.

[18] N. N. Sakhare, R. Kulkarni, N. Rizvi, D. Raich, A. Dhablia, and S. P. Bendale. A Decentralized Approach to Threat Intelligence using Federated Learning in Privacy-Preserving Cyber Security. 2023.

[19] A. Tabassum, A. Erbad, W. Lebda, A. Mohamed, and M. Guizani. FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. Comput Commun. 2022;192(1): 299-310.

[20] R. Doriguzzi-Corin and D. Siracusa. FLAD: Adaptive Federated Learning for DDoS attack detection. Comput Secur. 2024; 137 (1):103.

[21] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis. PPFL: privacy-preserving federated learning with trusted execution environments. In Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services. New York, NY, USA: ACM. 2021:94-108.

[22] P. Thantharate and T. Anurag. CYBRIA - Pioneering Federated Learning for Privacy-Aware Cybersecurity with Brilliance. In 2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT. HONET. 2023.

[23] M. D. Bergren. HIPAA-FERPA REVISITED. The Journal of School Nursing. 2004; 20(2): 107-112.

[24] H. Li, L. Yu, and W. He. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management. 2019; 22(1):1-6.

[25] P. F. Edemekong, P. Annamaraju, M. Afza, and M. J. Haydel. Health Insurance Portability and Accountability Act (HIPAA) Compliance. National Library of Medicine. 2024.

[26] S. Boudko. Federated Learning for Collaborative Cybersecurity of Distributed Healthcare. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023.