Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.13 No.2, 2024, pp.67-72

www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2024.13.2.4303

Adaptive and Privacy-Preserving Security for Federated Learning Using Biological Immune System Principles

Mobolaji Olusola Olarinde*, Akeem Adekunle Abiona and Micheal Olalekan Ajinaja
Department of Computer Science, Federal Polytechnic Ile-Oluji, Nigeria
E-mail: akeabiona@fedpolel.edu.ng, micajinaja@fedpolel.edu.ng
*Corresponding Author: mobolarinde@fedpolel.edu.ng
(Received 22 September 2024; Revised 22 October 2024, Accepted 13 November 2024; Available online 16 November 2024)

***Abstract* - The increasing frequency and sophistication of cyber threats pose significant challenges to the security of distributed systems handling sensitive data. Federated learning, a decentralized machine learning framework, enables collaborative model training without sharing raw data, offering privacy advantages. However, ensuring the security and resilience of federated learning systems remains a pressing concern due to potential vulnerabilities, such as data poisoning and model inversion attacks. This study aims to enhance the security of federated learning systems for website threat intelligence by leveraging nature-inspired principles from biological immune systems. The objective is to design a robust and adaptive framework that addresses evolving cyber threats while preserving data privacy. A security framework was proposed, inspired by the adaptive and self-defensive mechanisms of biological immune systems. Key components include adaptive anomaly detection, dynamic threat response, and privacy-preserving mechanisms. The system architecture was validated using simulated federated learning environments, where machine learning algorithms and differential privacy techniques were employed to monitor and respond to threats in real time. The proposed system demonstrated effective detection of anomalies such as data poisoning and model inversion attacks, achieving high accuracy and low false-positive rates. The dynamic threat response mechanism mitigated potential risks by isolating compromised nodes and restoring model integrity. Privacy-preserving measures, including differential privacy and secure multi-party computation, ensured that sensitive data remained protected during the training process. The nature-inspired approach provided a robust, adaptive solution for enhancing the security of federated learning systems. By mimicking the immune system's ability to detect and respond to threats, the proposed framework improves resilience against evolving cyber threats, making it suitable for securing sensitive applications such as website threat intelligence. This study highlights the potential of biological principles in addressing modern cybersecurity challenges while safeguarding data privacy.**

***Keywords:* Federated Learning, Cyber Threats, Data Poisoning, Privacy-Preserving Mechanisms, Biological Immune Systems**

I. INTRODUCTION

The rapid digitization of services and the increased dependency on online platforms have turned websites into popular targets for cyber threats. These threats have become more complex and frequent as attackers employ advanced methods and techniques to exploit vulnerabilities, steal sensitive information, and disrupt operations. Common types of attacks include Distributed Denial of Service (DDoS), SQL injections, cross-site scripting, and phishing. While this has opened up the possibility of reaching a more global audience, it has also necessitated the implementation of robust threat intelligence systems to identify and mitigate these attacks in real time. In machine learning applied to cybersecurity, federated learning has emerged as a promising solution. It enables several parties to jointly train a global machine learning model without sharing raw data, thus preserving privacy and maintaining data protection regulations [1]. On the other hand, this decentralized method means every participant or client trains a model locally on its dataset and shares only the updates—namely the gradients—with a central server, which aggregates the updates to tune the global model. This approach is particularly useful when data contains sensitive information, such as in healthcare, finance, or cybersecurity, where disclosing raw data can result in significant privacy risks.

However, federated learning is not free of security issues. One of the major concerns is data poisoning, where malicious clients intentionally inject incorrect or misleading data into the training process to corrupt the global model [2]. Another threat is model inversion, which involves adversaries using access to a model's parameters or outputs to reconstruct sensitive input data, effectively breaching the privacy that federated learning aims to protect [3]. Additionally, intercepted communication between clients and the central server may also risk data privacy, allowing attackers to eavesdrop or manipulate model updates for their own purposes, which can compromise model integrity [4]. Therefore, there is an urgent need for innovative security mechanisms to protect these systems from such threats.

In this paper, we propose integrating nature-inspired security mechanisms, particularly those from the biological immune system, to improve resiliency in federated learning for website threat intelligence. The immune system is a highly adaptive and self-defensive system capable of detecting and neutralizing foreign invaders in real time [5]. Our approach introduces dynamic anomaly detection and adaptive response mechanisms by emulating these characteristics. These mechanisms aim to detect and respond to potential threats more rapidly while preserving data integrity and privacy.

The rest of this paper is organized as follows: Section 2 reviews relevant literature on nature-inspired computing and security in federated learning. Section 3 presents an analogy between the immune system and the proposed security framework. Section 4 describes the architecture of the proposed system, while Section 5 discusses the implementation and experimental setup. Section 6 presents the results and discussion, and Section 7 concludes with a summary of the findings and suggestions for future work.

II. REVIEW OF LITERATURE

The security of federated learning systems has been an area of active research, given the growing adoption of this decentralized approach in various sensitive domains. Several strategies have been proposed to address the unique security challenges associated with federated learning, ranging from cryptographic techniques to nature-inspired approaches.

A. Federated Learning Security

Ensuring the integrity and privacy of the data used to train the global model is one of the key concerns in federated learning. To address this, homomorphic encryption and secure multi-party computation (SMPC) are among the various cryptographic techniques that have been proposed. In homomorphic encryption, operations can be performed directly on encrypted data without decryption, thereby ensuring the protection of privacy throughout the learning process [6]. In contrast, SMPC allows multiple parties to jointly evaluate a function on their inputs in such a way that the inputs remain private [7]. While these techniques provide good solutions to prevent data disclosure, they are often accompanied by high computational overhead, which may become a bottleneck in large-scale implementations.

Complementary to cryptographic techniques, differential privacy has gained broad acceptance in protecting the disclosure of individual data points' privacy in federated learning. Differential privacy injects random noise into model updates before sharing them with a central server to ensure that the presence or absence of any single data point does not significantly influence the output of the model [8]. While differential privacy provides a robust privacy guarantee, the added noise can sometimes result in degraded accuracy, creating a trade-off between privacy and performance.

Despite these advances, federated learning systems remain vulnerable to data poisoning and model inversion attacks. Data poisoning attacks involve malicious participants who inject false data during training, thereby corrupting the global model. Several proposed defenses, such as robust aggregation methods that detect and exclude outlier updates [9], are usually reactive, detecting attacks after they have occurred. Model inversion attacks are another significant threat, where an adversary seeks to reconstruct sensitive input data from the model parameters or outputs. To mask the internal representations of the model, a few techniques, such as gradient masking and regularization, have been attempted; however, these also affect the learning efficiency of the model [10].

B. Nature-Inspired Security Approaches

Nature-inspired computing, based on principles and mechanisms of natural systems, has become increasingly popular as a new paradigm for security enhancement in a wide range of domains, including federated learning. Among these, artificial immune systems (AISs), which successfully emulate the adaptive and self-defensive features of biological immune systems, have had a particularly strong influence. AIS has also been applied to various cybersecurity applications, including intrusion detection systems and anomaly detection, due to its ability to adaptively learn and recognize novelty [11]. In this context, AIS-inspired methods could provide dynamic and adaptive security measures within federated learning. For example, the work of Hofmeyr and Forrest on AIS architecture represents an application of immune system principles for anomaly detection in distributed systems through patterns that do not conform to the norm [12]. This adaptive capability is crucial in federated learning, as the system must monitor and respond to potential threats in real-time continually. By integrating AIS into federated learning, a system can proactively detect and neutralize threats before they compromise the integrity of the model or the privacy of the participants.

Another related nature-inspired method is swarm intelligence, based on the collective behavior of decentralized, self-organized systems, such as ant colonies or flocks of birds. Swarm intelligence has been applied to optimize security protocols in distributed networks by providing autonomous and coordinated responses to threats [13]. Although swarm intelligence is considered promising for enhancing resilience in distributed systems, its application in the security of federated learning is relatively unexplored compared to AIS.

C. Integration of Nature-Inspired Techniques in Federated Learning

Recent studies have begun exploring the integration of nature-inspired techniques into federated learning to address its inherent security challenges. For example, Chen et al. proposed a hybrid approach combining differential privacy with artificial immune systems (AIS) to enhance the privacy and security of federated learning systems. Their method demonstrated improved resistance to data poisoning attacks while maintaining model accuracy [14]. However, the study primarily focused on privacy aspects, leaving room for further exploration into how AIS can be leveraged to counteract other types of attacks, such as model inversion or communication interception. Similarly, Xia et al. developed a federated learning framework incorporating swarm intelligence principles to enhance the system's robustness against distributed denial-of-service (DDoS) attacks. Their approach showed potential in improving the system's

resilience to large-scale network disruptions, although its effectiveness against subtler attacks, like model inversion, has yet to be fully evaluated [15].

The integration of nature-inspired techniques into federated learning security is a promising area of research that combines the strengths of biological systems with the latest advancements in machine learning. While existing studies have made significant progress, there is still considerable potential for further development, particularly in creating holistic security frameworks that address the full spectrum of threats in federated learning environments.

III. ANALOGIES BETWEEN THE IMMUNE SYSTEM AND THE PROPOSED SECURITY FRAMEWORK

The immune system in biological organisms is a highly sophisticated and adaptive defense mechanism that continuously monitors the body for signs of infection and responds to potential threats in real time. This system operates through a complex network of cells, tissues, and organs that work together to identify, neutralize, and remember foreign invaders, such as bacteria, viruses, and other pathogens. The immune system's ability to distinguish between self and non-self, adapt to new threats, and maintain homeostasis is particularly relevant when considering the design of security frameworks for federated learning systems.

A. Adaptive Immunity and Dynamic Threat Detection

Adaptive immunity is considered one of the main components of the immune system, allowing the body to recognize specific pathogens and remember them. Adaptive immunity has the unique capability to learn from past infections and mount a more effective response upon subsequent exposures to the same pathogen. This is similar to how a federated learning system must identify and react to cyber threats that change over time, learning from past experiences to reinforce its defense mechanisms. In our proposed security framework, we draw inspiration from adaptive immunity for the realization of dynamic threat detection within a federated learning environment. Just as the human immune system utilizes various cell types, including T cells and B cells, each responsible for recognizing specific antigens and mounting an effective response, our framework uses anomaly detection algorithms that identify unusual patterns in model updates submitted by participants. These algorithms are designed to evolve over time and enhance their precision in threat detection based on the novelties of attacks that the system faces. This adaptive capability is crucial in a federated learning system because the nature of cyber threats may evolve, and static security measures may fail to withstand them [16].

B. Anomaly Detection and Threat Neutralization

The immune system's ability to detect and neutralize pathogens before they cause significant harm is a key aspect of its effectiveness. This process involves identifying foreign invaders (antigens) and subsequently activating immune responses to neutralize them. In the context of federated learning, anomaly detection serves a similar purpose by identifying malicious activities, such as data poisoning or model inversion attempts, that deviate from normal behavior. In our security framework, the anomaly detection module is inspired by the immune system's recognition processes. This module continuously monitors the updates provided by each participant in the federated learning system, looking for signs of anomalous behavior that could indicate an ongoing attack. When a potential threat is identified, the system activates a threat-neutralization response, analogous to the immune system's activation of immune cells to combat pathogens. This response may involve isolating the suspicious participant, re-evaluating the affected model updates, or deploying countermeasures to prevent the spread of the threat within the network [17].

C. Self-Non-Self Discrimination and Privacy Preservation

A fundamental attribute of the immune system is its ability to distinguish between self and non-self, targeting only the injurious foreign invaders for destruction while leaving the host's own cells intact. This concept is crucial in a federated learning system, where data privacy and integrity must be protected for the participants while securing the entire system against external threats. Our proposed framework integrates a privacy-preserving mechanism that aligns with the self-non-self-discrimination of the immune system, ensuring that security measures do not breach the privacy of individual participants. Differential privacy and secure multi-party computation are employed to obfuscate sensitive data while maintaining the system's effectiveness in threat detection and response [18]. The clear distinction it makes between benign and malicious activities allows genuine participants to cooperate in the federated learning process with confidence that there will be no compromise in data security or misuse.

D. Memory and Continuous Learning

Another key feature of the immune system is the memory it provides, wherein the body responds much faster and stronger upon the re-invasion of pathogens that have previously infected it. This memory develops after the initial immune response and serves as the basis for immunity against recurrent infections. Similarly, our security framework is complemented by the continuous learning feature, which enables the system to remember past attacks and take into consideration the development of future responses. The system can keep a log of the threats detected and the efficiency of their respective neutralization methods for further improvements in threat detection and neutralization. This continuous learning process is vital for staying ahead of adversaries in the ever-changing landscape of cyber threats [19]. The analogy between the immune system and our proposed security framework for federated learning shows the potential of nature-inspired approaches to enhance the resilience of distributed systems. The adaptive,

self-defensive, and memory-driven properties of the immune system are emulated by the framework to provide a strong and dynamic security solution capable of protecting federated learning environments from a wide range of cyber threats. This approach not only addresses the deficiencies of current security methods but also lays the groundwork for more advanced defense strategies in the future.

IV. ARCHITECTURE OF THE PROPOSED SYSTEM

The concept of the security framework in federated learning is inspired by the biological immune system, with the purpose of enhancing resilience against evolving cyber threats in distributed machine learning models. The architecture integrates adaptive anomaly detection, dynamic threat response, and privacy-preserving mechanisms for security and privacy assurance in federated learning environments. The main components of the proposed system architecture include the following:

1. *Local Model Training Nodes:* Each client participating in federated learning will train a local machine learning model on their data. These clients do not share their raw data but broadcast model updates - such as gradients - to a central server. Each client node is thus equipped with a local anomaly detection module that observes the integrity of data and the training process.
2. *Central Aggregation Server:* The central server aggregates the model updates received from the participating clients to form the global model. This server also hosts the core components of the proposed security framework, including the global anomaly detection module, the threat response module, and the privacy-preserving mechanisms.
3. *Global Anomaly Detection Module:* The module is designed to constantly monitor model updates from the clients for any deviation or anomaly, drawing inspiration from the pattern recognition ability of the human immune system. It will make use of statistical analysis combined with machine learning techniques to identify patterns indicative of an attack—such as poisoning or model inversion attempts.
4. *Dynamic Threat Response Module:* The dynamic threat response module is triggered once a potential threat is detected. It evaluates the severity of the anomaly and deploys necessary countermeasures, such as isolating the suspicious client, reverting the global model to one of its earlier states, or re-weighting the contributions of the different clients to reduce the impact of the detected anomaly.
5. *Privacy-Preserving Mechanisms:* Differential privacy techniques and secure multi-party computation methods are incorporated into the system so that security measures do not compromise individual participant privacy. These mechanisms mask or distort sensitive data while maintaining the system's capability to accurately perform anomaly detection and threat response. Differential privacy achieves this by adding noise to model updates before aggregation, while the SMPC approach ensures that the central server cannot access the raw data from any particular client.
6. *Memory and Continuous Learning Module:* This module records each detected threat and the corresponding responses, much like the immune system's memory, enabling the system to continuously learn from incidents. The historical data is used to refine the algorithms for anomaly detection, thereby enhancing the system's ability to respond to new threats.

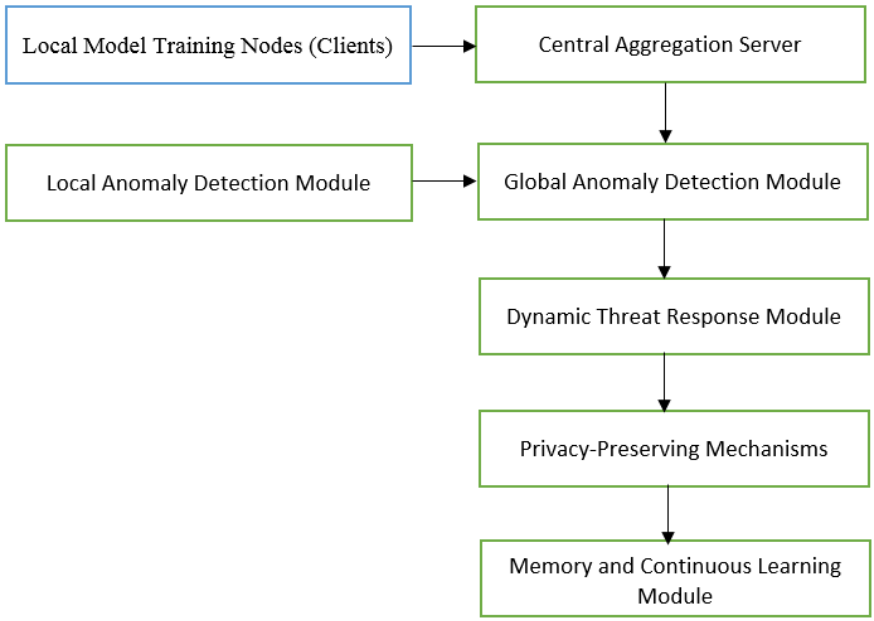

Fig. 1 Architecture of the proposed framework

Figure 1 provides a visual representation of the architecture for the proposed federated learning security framework. The diagram illustrates the key components, including the local model training nodes (clients), anomaly detection modules,

the central aggregation server, and the various security mechanisms integrated into the system. The arrows indicate the flow of information and how different modules interact within the framework.

A. System Workflow of the Proposed Framework

The system workflow in the proposed federated learning security framework ensures continuous protection against cyber threats while maintaining model accuracy and data privacy. The workflow follows these key steps:

1. *Initial Model Training:* Each client independently trains its local model on its dataset, ensuring that sensitive data never leaves the client's environment.
2. *Model Update Submission:* Once the local training is complete, clients submit their model updates (e.g., gradients) to a central aggregation server. Before submission, local anomaly detection checks the updates for any irregularities.
3. *Global Anomaly Detection:* The updates at the central server from all clients are fed into a global anomaly detection module for processing. This module searches for suspicious patterns that may signify potential threats, including poisoning and malicious model inversion.
4. *Dynamic Threat Response (if necessary):* The dynamic threat response module is triggered if the global anomaly detection module flags updates as suspicious. This module will take appropriate action, which may involve isolating the client, rolling back the global model to the previous state, or adjusting the weights of the model updates to invalidate the detected threat.
5. *Model Aggregation and Update:* The server aggregates the validated updates of models to form the new global model after mitigating any threats. This updated model reflects the contributions of all legitimate clients while excluding or correcting any compromised data.
6. *Continuous Learning:* The threats detected, along with their respective responses, are logged into the system continuously to further enhance anomaly detection algorithms and threat response strategies. This ensures the system becomes more resilient over time.
7. *Return to Clients:* The updated global model is then returned to the clients, who use it as a starting point for the next round of local training.

This workflow provides a secure, adaptive, and privacy-preserving federated learning process, making it robust against a wide range of cyberattacks.

B. Data Flow of the Proposed Framework

In this section, we describe the data flow for implementing a nature-inspired security approach based on the immune system to enhance federated learning systems for threat intelligence in websites. The proposed approach leverages mechanisms inspired by the biological immune system, such as anomaly detection and adaptive threat response, to secure data and model updates within the federated learning framework.

1. *Initialization Phase:* The Federated Nodes Initialization is the first step. Each federated node (e.g., website server) is initialized with a local machine learning model designed for threat intelligence. Anomaly detection and response mechanisms, inspired by the immune system, are integrated into each node. A global model is established at the central aggregator. This model is initialized with a baseline configuration, which will be refined based on the aggregated updates from the federated nodes.
2. *Local Training and Data Processing:* Each node collects and processes local data related to website traffic and potential threats. This data includes various attributes, such as user behavior, access patterns, and known threat signatures. Nodes train their local models using the collected data. During training, the immune-inspired security mechanism monitors for anomalies and potential threats. The anomaly detection mechanism, modeled after the immune system's ability to recognize foreign invaders, continuously scans for unusual patterns or deviations from expected behavior.
3. *Threat Response:* If anomalies or potential threats are detected, the adaptive threat response mechanism initiates predefined actions, such as isolating affected data or enhancing local model defenses.
4. *Model Update and Communication:* After local training, each node generates updates (e.g., model parameters or gradients) to improve the global model. These updates include information about detected anomalies and the corresponding responses. The updates are transmitted securely to the central aggregator. The immune-inspired system ensures that communication channels are protected against potential interception or tampering.
5. *Aggregation and Integration:* The central aggregator collects model updates from all federated nodes. During aggregation, the system verifies the integrity of the received updates and assesses the security implications of the included anomaly and threat response data. The global model is updated based on the aggregated updates. The updated model incorporates improvements and responses to detected threats, enhancing its ability to identify and address emerging threats.
6. *Feedback and Adaptation:* The performance of the global model and security mechanisms is assessed. This involves detection accuracy, response effectiveness, and overall system resilience. Based on the evaluation results, the system then adjusts the mechanisms of anomaly detection and threat response. By adapting to new threats and evolving attack patterns, the system refines its security measures and model parameters. The refined global model is then redistributed back to the federated nodes. Each node combines the updated model, adapting it to its anomaly detection and response mechanisms.
7. *Continuous Monitoring and Updates:* The system continues to monitor the performance of both the federated learning models and the security mechanisms. Continuous feedback ensures that the approach remains effective against emerging cyber threats. Regular

updates to the models and security mechanisms are performed to maintain robustness and adaptability in the face of evolving threats.

V. CONCLUSION

In light of the increasing sophistication of cyber threats, protecting the security and privacy of sensitive data in distributed environments has made the protection of federated learning systems imperative. This paper proposes a novel, nature-inspired approach to enhancing the security of federated learning systems for threat intelligence in websites, using adaptive and self-defensive mechanisms of the biological immune system. Our approach embeds robust security in the federated learning environment by leveraging the dynamic and self-organizing properties of the immune system. By embedding dynamic anomaly detection and adaptive threat response mechanisms, we enable the system to spot and mitigate potential threats in real-time while maintaining the integrity and confidentiality of the distributed data. The bio-inspired methodology presented here has made significant advances in addressing the unique security challenges intrinsic to federated learning systems. The embedding of immune mechanisms in the design of federated learning frameworks adds significant levels of security, adaptability, and resilience—fundamental to addressing the dynamic nature of threats in cyberspace. By demonstrating how nature-inspired methods can provide creative solutions to complex security issues, the proposed method unlocks possibilities for more secure and efficient federated learning systems. Future research will continue to refine adaptive security mechanisms, explore further nature-inspired models, and validate the proposed approach through extensive real-world testing. We have drawn inspiration from natural systems while developing and improving federated learning, contributing to the design of resilient distributed learning environments.

REFERENCES

[1] A. Elgabli, J. Park, S. Ahmed, and M. Bennis, "L-FGADMM: Layer-Wise Federated Group ADMM for Communication Efficient Decentralized Deep Learning," in *Proc. 2020 IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, Korea (South), 2020, pp. 1-6, doi: 10.1109/WCNC45663.2020.9120758.

[2] L. Miao, W. Yang, R. Hu, L. Li, and L. Huang, "Against Backdoor Attacks in Federated Learning with Differential Privacy," in *Proc. ICASSP 2022 - 2022 IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Singapore, 2022, pp. 2999-3003, doi: 10.1109/ICASSP 43922.2022.9747653.

[3] X. Yan, B. Cui, Y. Xu, P. Shi, and Z. Wang, "A Method of Information Protection for Collaborative Deep Learning under GAN Model Attack," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 18, no. 3, pp. 871-881, May-Jun. 2021, doi: 10.1109/TCBB.2019.2940583.

[4] Y. Chen, X. Sun, and Y. Jin, "Communication-Efficient Federated Deep Learning With Layerwise Asynchronous Model Update and Temporally Weighted Aggregation," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 10, pp. 4229-4238, Oct. 2020, doi: 10.1109/TNNLS. 2019.2953131.

[5] V. Golovko, M. Komar, and A. Sachenko, "Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers," in *Proc. 2010 Int. Conf. Modern Problems Radio Eng., Telecommun. Comput. Sci. (TCSET)*, Lviv, Ukraine, 2010, pp. 237-237.

[6] M. R. Kumar and V. Lakshmipraba, "Hybrid Privacy Preserving Mechanism: An Approach to Protect Health Care Data," *Asian Journal of Computer Science and Technology,* vol. 7, no. 1, pp. 71-78, Feb. 2018.

[7] C. Hu, S. Wang, C. Liu, and T. Zhang, "Efficient Privacy-Preserving Data Aggregation for Lightweight Secure Model Training in Federated Learning," in *Proc. 2023 7th Int. Conf. Cryptogr., Security Privacy (CSP)*, Tianjin, China, 2023, pp. 119-123, doi: 10.1109/CSP58884. 2023.00026.

[8] S. Selvam, "A New Algorithm for Pattern Based Using Mining Association Rules," *Asian Journal of Computer Science and Technology,* vol. 9, no. 2, pp. 24-27, Aug. 2020.

[9] P. R. Kumar, S. Ravichandran, and N. Satyala, "Deep Learning Analysis: A Review," *Asian Journal of Computer Science and Technology,* vol. 7, no. S1, pp. 24-28, Oct. 2018.

[10] B. Fang and T. Zhang, "Deeper Leakage from Gradients through Membership Inference Attack," in *Proc. 2024 7th Int. Conf. Inf. Comput. Technol. (ICICT)*, Honolulu, HI, USA, 2024, pp. 295-300, doi: 10.1109/ICICT62343.2024.00054.

[11] T. Gong, "Artificial Immune System Based on Normal Model and Immune Learning," in *Proc. 2008 IEEE Int. Conf. Syst., Man, Cybern.*, Singapore, 2008, pp. 1320-1325, doi: 10.1109/ICSMC.2008.4811468.

[12] M. B. A. Hamid and T. K. A. Rahman, "Short Term Load Forecasting Using an Artificial Neural Network Trained by Artificial Immune System Learning Algorithm," in *Proc. 2010 12th Int. Conf. Comput. Modelling Simulation*, Cambridge, UK, 2010, pp. 408-413, doi: 10.1109/UKSIM.2010.82.

[13] P. Dewangan and Neelamsahu, "A Proposed Method for Mining Breast Cancer Pattern Using Particle Swarm Optimization," *Asian Journal of Computer Science and Technology,* vol. 8, no. 1, pp. 69-73, Feb. 2019.

[14] W. Yuwen, G. Yu, and L. Xiangjun, "Differential Privacy Hierarchical Federated Learning Method Based on Privacy Budget Allocation," in *Proc. 2023 9th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, 2023, pp. 2177-2181, doi: 10.1109/ICCC59590.2023.10507299.

[15] V. Subrahmanyam, V. Janaki, P. S. Rao, N. Gurrapu, S. K. Mandala, and R. Roshan, "Internet of Things (IoT) Based Data Analysis for Feature Selection by Hybrid Swarm Intelligence (SI) Algorithm," in *Proc. 2024 IEEE Int. Conf. Interdiscip. Approaches Technol. Manag. Social Innov. (IATMSI)*, Gwalior, India, 2024, pp. 1-6, doi: 10.1109/ IATMSI60426.2024.10503278.

[16] R. R. Ema and P. C. Shill, "Integration of Fuzzy C-Means and Artificial Neural Network with Principal Component Analysis for Heart Disease Prediction," in *Proc. 2020 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225366.

[17] M. Hassan, M. A. Butt, and M. Z. Baba, "Logistic Regression Versus Neural Networks: The Best Accuracy in Prediction of Diabetes Disease," *Asian Journal of Computer Science and Technology,* vol. 6, no. 2, pp. 33-42, Sep. 2017.

[18] J. Xu, Z. Ning, Y. Zhou, X. Liao, W. Zou, and S. Xing, "An Indoor Localization Mechanism Based on Local Differential Privacy," in *Proc. 2023 4th Inf. Commun. Technol. Conf. (ICTC)*, Nanjing, China, 2023, pp. 121-126, doi: 10.1109/ICTC57116.2023.10154748.

[19] M. B. Fathima Sanjeetha, Y. Kanagaraj, V. Herath, and S. Lokuliyana, "Deep Learning for Edge Computing Applications: A Comprehensive Survey," *Asian Journal of Computer Science and Technology,* vol. 11, no. 2, pp. 39-47, Nov. 2022.