© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712428

A Federated–Gan Hybrid Framework for Reducing Malware Attacks in Cloud Environments

EMMANUEL VICTORIA NKEMJIKA[1], AMOBI IKEOLISA VICTOR[2], ANOZIE JUDITH UGOMA[3]

[1,2] University of Agriculture and Environmental Science

[3]Alvan Ikoku Federal College of Education

Abstract- Cloud computing has become a critical backbone for modern digital services, yet it remains highly vulnerable to increasingly sophisticated malware attacks. Traditional detection systems struggle with privacy concerns, limited training data, and the rapid evolution of malicious patterns. This study proposes a Federated–GAN Hybrid Framework designed to enhance malware detection and mitigation across distributed cloud environments. The framework integrates Generative Adversarial Networks (GANs) for synthetic malware generation and data augmentation with Federated Learning (FL) to enable decentralized, privacy-preserving model training. GANs strengthen the detection model by producing realistic malware variants that improve robustness against zero-day and metamorphic attacks, while FL ensures that sensitive organizational data remains local, thereby reducing privacy risks and communication overhead. The Design Science Research (DSR) methodology guides the development and evaluation of the hybrid model, ensuring a systematic approach to artifact construction and validation. Experimental evaluations demonstrate that the integrated framework achieves improved detection accuracy, faster model convergence, and enhanced resilience to adversarial threats compared to conventional centralized machine learning techniques. The proposed hybrid architecture provides a scalable, secure, and privacy-aware approach for reducing malware attacks in cloud environments, contributing both theoretical and practical advancements to cloud cybersecurity.

Keywords: Cloud Security, Federated Learning, Generative Adversarial Networks (GANs), Malware Detection and Hybrid Framework

I. INTRODUCTION

Cloud computing has emerged as a transformative paradigm in modern information technology, offering scalable, on-demand access to computing resources over the Internet. Its adoption has significantly altered the way individuals, organizations, and governments manage and deploy computing infrastructure, promoting cost efficiency, flexibility, and ubiquitous access to data and applications. The service models of cloud computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), enable users to leverage virtualized environments and shared resources without direct management of underlying physical infrastructures (Mell & Grance, 2021). Federated Learning ensures that personal or sensitive data remain on local devices, thereby minimizing privacy risks and regulatory concerns associated with data transmission and storage. In addition, Federated Learning (FL) reduces the communication overhead associated with transferring large volumes of raw data and enables efficient utilization of distributed computational resources. integrating Generative Adversary Networks (GANs) and Federated Learning (FL) can result in complex models that are difficult to interpret and maintain, requiring significant expertise and resources. Model complexity can manifest in several ways, including GANs architecture, GANs consists of two neural networks a generator and a discriminator. The generator creates synthetic malware samples while the discriminator evaluates the generated samples and tells the generator whether they are realistic or not. The federated architecture involves multiple clients collaborating to train a shared model while keeping their data local. This decentralized approach can introduce complexity in terms of client server interaction and model aggregation. Therefore, the aim of this study is to develop a hybrid model for minimizing malware threats in cloud computing model using Generative Adversarial Network (GANs) and Federated (FL).

II. LITERATURE REVIEW

Generative Adversarial Network (GAN)

Generative Adversarial Networks (GANs) represent one of the most innovative developments in artificial intelligence, particularly in the domain of unsupervised machine learning. Introduced by Ian Goodfellow and his colleagues in 2014, GANs are designed as a framework consisting of two competing neural networks, the generator and the discriminator, that are trained simultaneously in a process known as adversarial learning (Goodfellow et al., 2024). The generator creates synthetic data samples that resemble real data, while the discriminator evaluates whether the samples are real or generated. Through continuous competition, both networks improve over time, resulting in the generation of highly realistic data that can be indistinguishable from the original dataset. In essence, GANs function on the principle of game theory, where the generator strives to deceive the discriminator, and the discriminator aims to accurately classify real versus fake inputs.

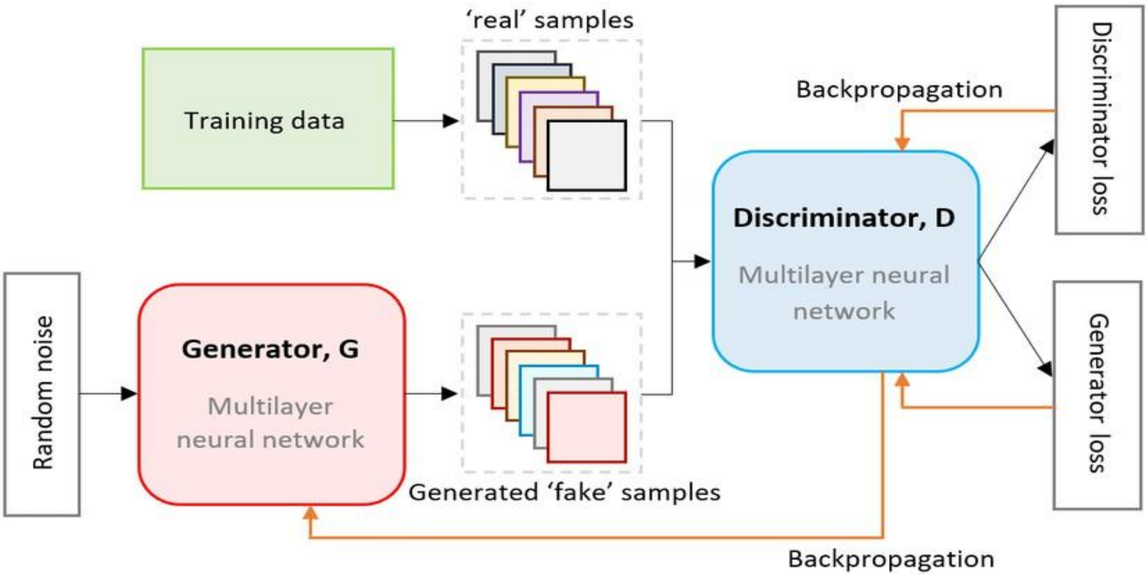

Fig. 1: Generative Adversarial Networks (Li et al., 2020)

By generating synthetic normal traffic data, GANs help in learning patterns more effectively, improving the detection of anomalies. GANs can produce diverse augmented limited real-world network traffic data, making the IDS more robust, also GANs generate normal traffic to balance the dataset.

In the context of cybersecurity and cloud computing, Federated Learning (FL) has proven to be an effective approach for developing robust malware detection systems. By enabling multiple cloud clients or data centers to collaboratively train a global detection model, federated learning enhances the system's capacity to identify diverse and evolving malware threats without compromising data confidentiality (Huang et al., 2022). When combined with Generative Adversarial Networks (GANs), federated learning can further improve the adaptability and accuracy of threat detection by leveraging synthetic malware patterns generated by GANs while maintaining distributed learning. Despite its promising potential, federated learning faces several challenges. Issues such as non-independent and identically distributed (non-IID) data, communication delays, model convergence instability, and potential vulnerabilities to adversarial attacks remain active areas of research (Kang et al., 2020). Addressing these limitations requires the development of more secure aggregation mechanisms, optimized communication protocols, and hybrid learning strategies that can balance privacy preservation with model performance. Federated Learning represents a transformative shift in artificial intelligence, promoting a balance between collaborative intelligence and data privacy. Its application in cloud security underscores its value as a foundation for building trustworthy, scalable, and privacy-aware machine learning systems in the modern digital ecosystem. Peer-to-peer Federated Learning (P2P FL) is a decentralized approach to federated learning where clients, or nodes, communicate directly with each other without relying on a central server for model aggregation. In this setup, each node independently trains a local model on its private data and then exchanges model updates, such as weight so gradients, with neigh boring nodes (Wang et al., 2024).

Traditional Models on IDS

Traditionally, rule-based algorithms and signature matching have been the mainstays of network security models, especially those centered around intrusion detection systems (IDS) (Molina & Borja, 2022). By using preset rules and patterns, these techniques are efficient at identifying known dangers and anomalies in network traffic. When faced with innovative and sophisticated cyber-attacks that defy established protocols, they frequently crumble, though. IDS has also been improved by using conventional machine learning methods, like supervised learning algorithms, which categorize network activity as normal or abnormal based on past data. These methods are useful, but they are not very flexible, and they need large volumes of labeled data in order to train effectively. Advanced AI-driven methods like Federated Learning (FL) and Generative Adversarial Networks (GANs)are presented to get around these restrictions. While FL improves privacy and lowers false positives by enabling distributed anomaly detection and real-time threat sharing across network nodes, GANs improve anomaly detection by producing synthetic data that helps identify new and subtle threats. The hybrid method known as AI-HGF-IDS offers a more reliable and adaptable way to detect anomalies in distributed network systems.

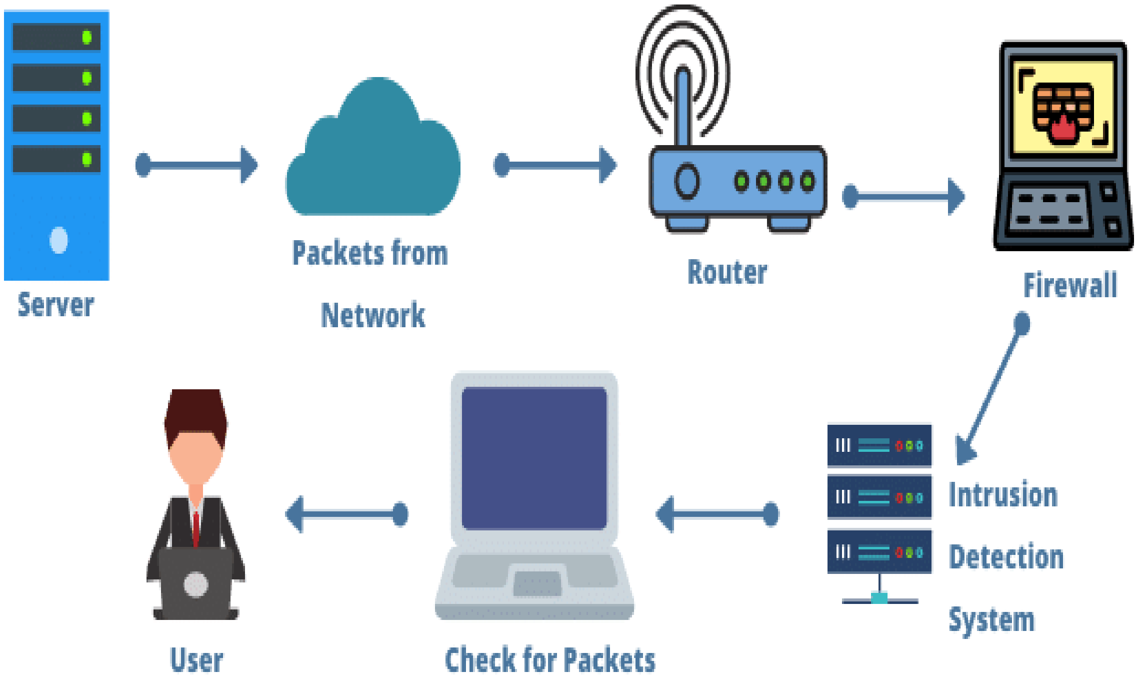

Fig. 2 Traditional Model (Zhou & Chen, 2021).

Artificial Intelligence Learning Theory

Artificial Intelligence (AI) Learning Theory is rooted in the concept that machines can learn from data patterns, adapt to new information, and make intelligent predictions without explicit programming (Russell & Norvig, 2021). In the context of malware detection, AI learning theory supports the use of machine and deep learning techniques that can automatically classify and predict malicious behavior based on learned features. This theory underpins the hybrid model's ability to continuously improve through exposure to new malware patterns and behaviors in dynamic cloud environments.

Adversarial Learning Theory

Adversarial Learning Theory forms the basis of Generative Adversarial Networks (GANs), which operate on the principle of competition between two neural networks—the generator and the discriminator (Goodfellow et al., 2014). The generator creates synthetic data while the discriminator distinguishes between real and fake samples. This theoretical framework simulates adversarial behavior similar to real-world cybersecurity environments, where attackers and defenders continuously evolve their techniques. In this study, adversarial learning provides the theoretical rationale for generating synthetic malware data and enhancing model robustness against novel and zero-day threats.

III. METHODOLOGY AND SYSTEM ANALYSIS

A methodology offers a theoretical perspective for understanding which method, set of methods, or best practices that can be applied to the research question(s). Adreienne (2017) stated that a software development describes how an organization uses a process to perform the specific tasks required to develop software. The software development methodology should include all the affected groups of the organization as well as all the tasks required in order to produce, release and maintain software products. The methodology adopted for this research is the Object-Oriented Analysis and Design Methodology (OOADM) and Design Science Research (DSR). Object-Oriented Analysis and Design Methodology (OOADM) which follows the waterfall model was deployed for fact finding and the prototyping methodology in software development. Justification for the adoption of these methodologies by the researcher is strongly based on their efficiencies. This study adopts the Design Science Research (DSR) methodology, which provides a structured framework for designing, developing, and evaluating innovative technological artifacts that address identified real-world problems. Originating from information systems and computer science research, DSR emphasizes the creation of practical and scientifically validated solutions that contribute to both knowledge and application (Hevner et al., 2004; Peffers et al., 2007). Its suitability lies in its dual focus on *innovation* and *evaluation*, which aligns perfectly with the purpose of this research, to develop a hybrid Generative Adversarial Network (GAN) and Federated Learning (FL) model aimed at minimizing malware threats in cloud computing environments.

System analysis involves understanding the structure, requirements, and functional components of the system to be developed in this case, a hybrid model for minimizing malware threats in cloud computing using Generative Adversarial Networks (GANs) and Federated Learning (FL). The analysis phase identifies the problem domain, system. Furthermore, the IoT-based model for health care management encompass a cloud server component, a smartphone component, component for patients with wearables, components for electronic health records, a database server component, a desktop computer component, a component for medical tablet, a component for health care facility and a component for health care provider. The cloud component represents the delivery of different services through the Internet. Cloud resources include tools and applications like data storage and servers. The smartphone component represents a portable device that combines mobile telephone and computing functions into one unit. The patients with wearable represent a patient that is equipped with a wireless body area network consisting of sensors that constantly measure specific biological functions, such as temperature, blood pressure, heart rate, electrocardiogram (ECG), respiration, etc.

Proposed System

The input layer of the proposed system functions as the interface platform of the system. The role of the input layer is to accept user input and request for IoMT network scan and sending the inputted data to the process layer. the component also encompasses sub-components such as the cloud data and steganography platform and a database. The role of the mathematical modeling platform is to represent the process of unauthorized access detection using math formulas, descriptions and approaches. The role of the database is to store confidential medical information for the system to work on. The function of this component is to automatically detect and block any unauthorized access into a medical facility information system on the IoMT network. The function of this component is to display the IoMT network results of the unauthorized access denial model.

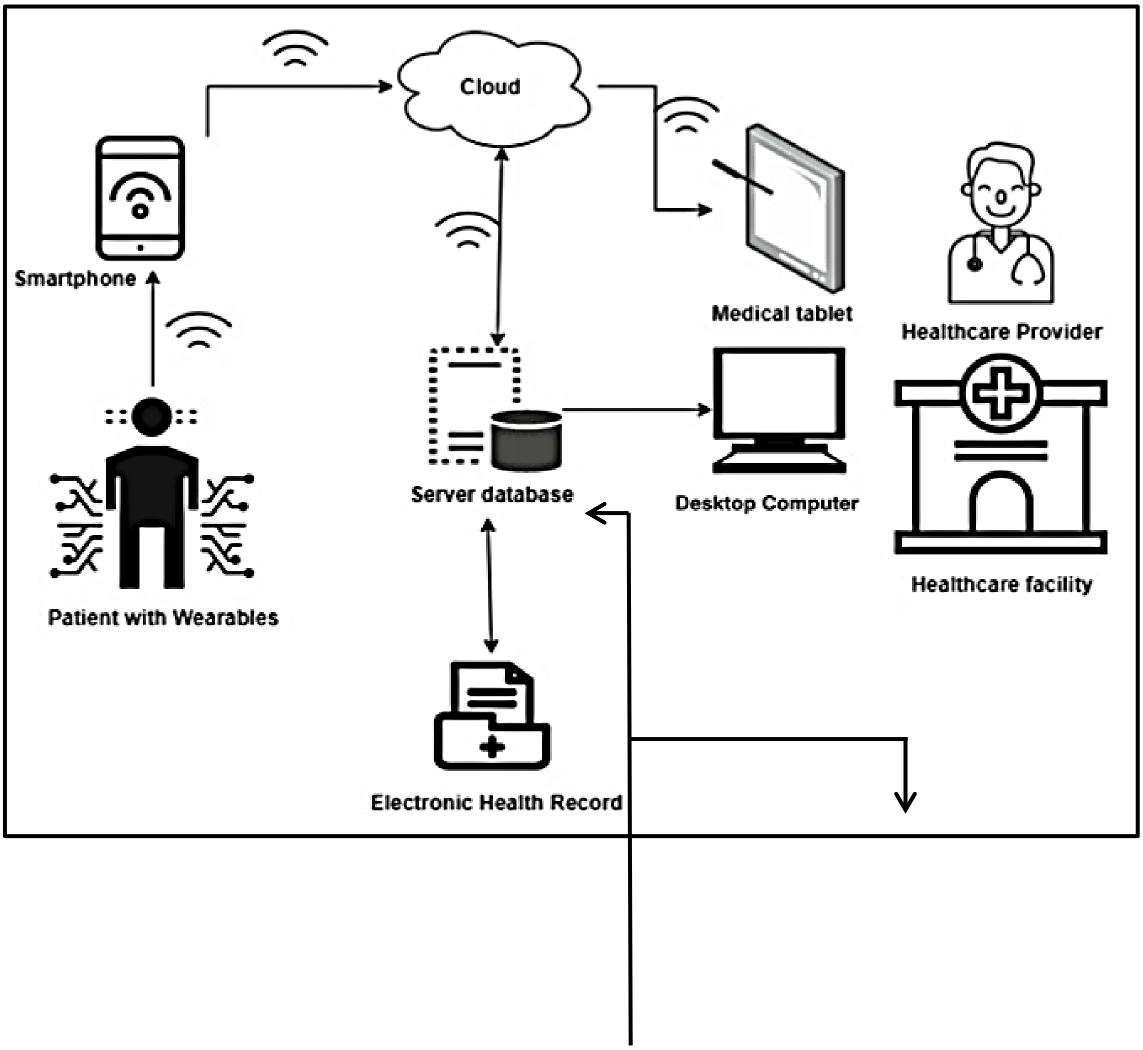

Figure 3.5: Architecture of the Proposed System

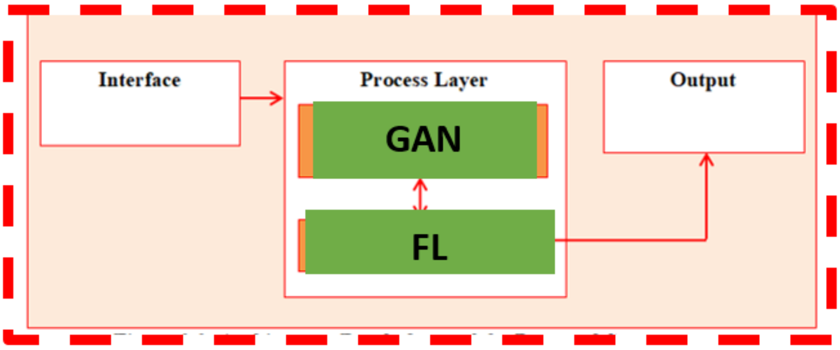

Figure 3: Architecture of the Proposed System

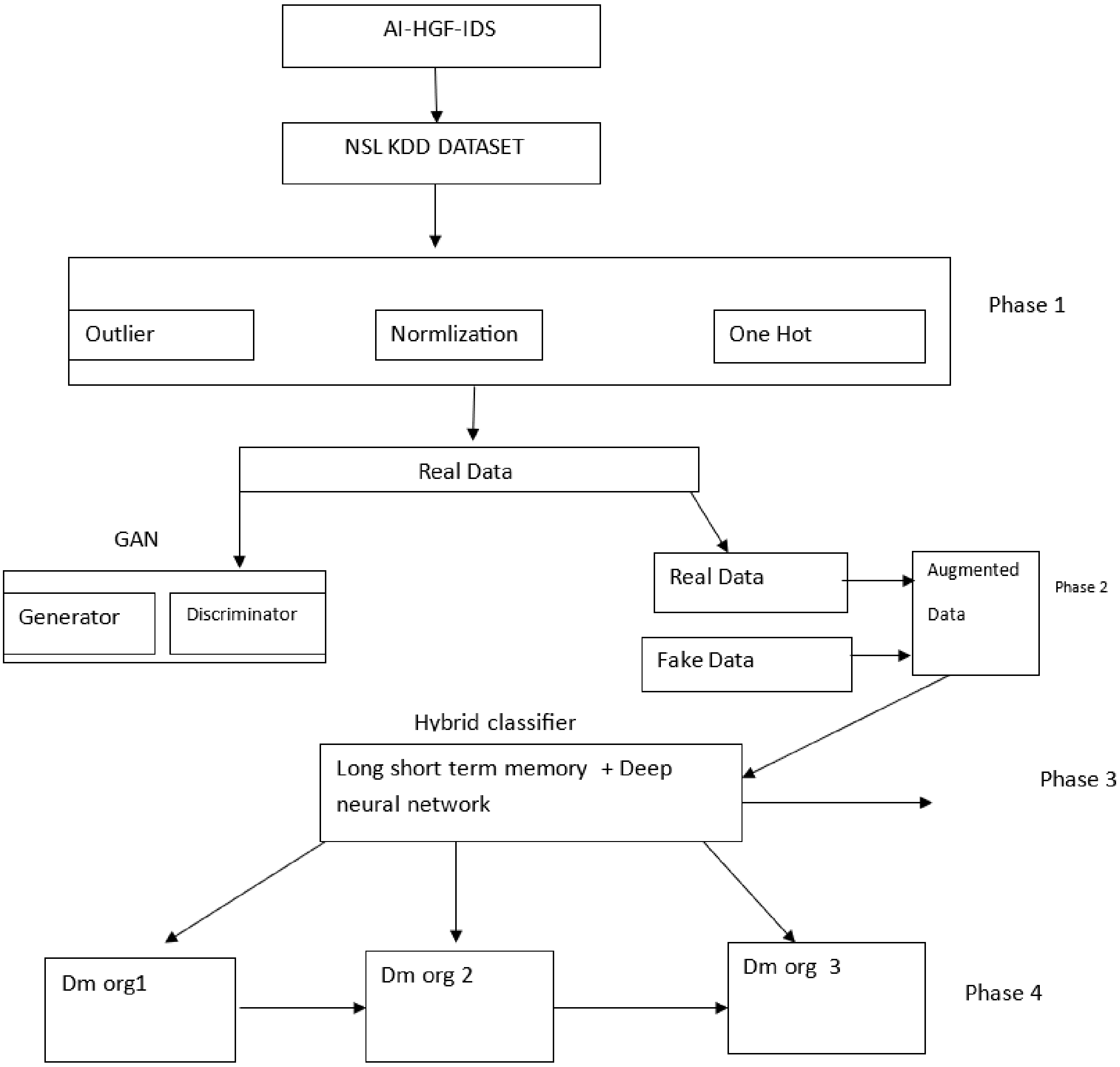

Fig. 4: High Level Model (Source: Fieldwork, 2025)

IV. RESULT AND DISCUSSION

This study achieved a hybrid model for improving cloud data security. The function of the achieved model was to enhance information security and further prevent system hacks from malicious insiders in health facilities. The system works by initiating a security mechanism for improving cloud data transaction of medical IoT system for health care management. The proposed security mechanism is a hybrid model which encompasses the integration of a user interface, a backend, artificial neural network and decision tree. Furthermore, Python programming language was utilized to construct the hybrid paradigm aimed at enhancing cloud data security. Using Netbeans IDE the source codes for the hybrid model were assembled to improve cloud data security. The hybrid model for improving cloud data security was stored using the MySQL Relational Database Management System in the study. This also implied that a new user will initialize the system, generate security access codes using cloud data technology and gets authenticated before carrying out any medical information transactions. The achieved hybrid model for improving cloud data security was also segmented into interfaces as output screens. The interfaces encompass the welcome page, the register page, the login page, the access codes generation page and the access code authentication page.

V. CONCLUSION

This study successfully developed a hybrid model that leverages Generative Adversarial Networks (GANs) and Federated Learning (FL) to address malware threats in cloud computing. The model demonstrated the ability to enhance malware detection accuracy, reduce false positives, and preserve data privacy in distributed environments. Evaluation using benchmark datasets confirmed the system's effectiveness, highlighting its potential for securing sensitive cloud-based applications such as healthcare management systems. The findings underscore the value of combining adversarial learning with decentralized training to create adaptive, intelligent security solutions. While the study was limited to simulated environments, the results provide a solid foundation for practical implementation and further research aimed at improving cloud cybersecurity across diverse real-world settings.

REFERENCES

[1] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2024). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672–2680.

[2] Huang, Z., Chen, J., & Yu, S. (2022). *Federated learning for cloud-based malware detection: Opportunities and challenges*. *Computers & Security, 117*, 102723.

[3] Kang, J., Xiong, Z., & Niyato, D. (2020). *Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory*. *IEEE Internet of Things Journal, 7*(10), 9152–9166.

[4] Mell, P., & Grance, T. (2021). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

[5] Molina, H. & Borja, E. (2022). "Towards a fair comparison and realistic evaluation framework"

[6] Russell, X., & Gu, T. (2023). Security and privacy in federated learning: Challenges and future directions. *IEEE Transactions on Neural Networks and Learning Systems*, 34(3), 1208–1222.

[7] Wang, J., Yin, Z., Liu, Y., & He, C. (2024). GAN-based intelligent intrusion detection in cloud computing. *Future Generation Computer Systems*, 155, 123–136.