iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.66108

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Federated AI for Cyber Defence: Enhancing Access Control Through Distributed Learning

Govindarajan Lakshmikanthan[1], Sreejith Sreekandan Nair[2]
[1, 2]*Independent Researcher, Leading Financial Firm, Texas, USA*

Abstract: ***System security and the protection of sensitive data has become a need of the hour as fast as the development of cyber threats. A federated Artificial Intelligence (AI) presents a distributed learning framework that handles these issues through the provision of secure collaboration that preserves data privacy. This paper explores how Federated AI can enhance access control systems by making them suitable for detecting anomalies, enforcing policies, and adapting to changing threats in real-time. Centralized AI models of the traditional sort necessitate data aggregation at a single location, an avenue open to any breach and compliance concerns. By training models over the federation of decentralized nodes, Federated AI mitigates these risks by allowing data locality. This paper presents a decentralized learning paradigm which implements robust access control mechanisms using collective intelligence and simultaneously keeps sensitive information safe. Additionally, the combination of Federated AI with Zero Trust principles leads to a dynamic access control system that changes with user behavior and the settings external to the user. We discuss key advancements such as the utilization of edge devices for real-time anomaly detection, privacy-based techniques such as differential privacy and homomorphic encryption, and the inclusion of generative models that simulate and predict attack scenarios. Finally, the paper underscores the advantages and limits of the potential of Federated AI in cyber defence.***

Keywords: Federated AI, Cybersecurity, Access Control, Anomaly Detection, Distributed.

I. INTRODUCTION

In today's more connected and decentralized world, organizations must keep up with annualized double-digit transformations in support of various digital initiatives. As cloud computing, remote work, and other distributed technologies gain traction, more manufacturers are adopting new operations models based on distributed systems. Despite the advantages of flexibility, scalability and low cost, these models introduce key cybersecurity issues. Naturally, these systems depend on strong access control mechanisms that only allow users to access the resources and data. [1-4] Unauthorized access is one of the biggest concerns, as it could lead to massive leaks, data theft, and the exposure of sensitive information. Increasing complexity in managing access control across organizational layers and geographically disparate locations compounds this, while compliance requirements for distributed service delivery and multiple forms of authentication continue to expand. With cyber threats becoming more sophisticated, traditional technologies focused on access control based on static process policies and centralized systems are inadequate. However, existing approaches are not easily scalable to the dynamic qualities of modern distributed environments where user roles, device types, and threat vectors constantly change. In this landscape, there needs to be innovative solutions to balance a strong security posture and, at the same time, comply with privacy regulations and protect sensitive data. A solution to that is Federated Learning (FL), a machine learning technique that enables entities (such as organizations or devices) to jointly train models without accessing each other's raw data. By distributing data processing and handling across several devices, federated learning reduces the risk associated with the concentration of data in central places. It offers a safer way to enhance cybersecurity in terms of access control.

A. The Need for Advanced Access Control Systems

In cybersecurity, access control is a fundamental aspect: who can access which resources and under what conditions. Traditional access control models such as Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC) have been used to some extent in a controlled environment. Yet, as organizations move toward more decentralized and dynamic systems, these traditional methods are becoming less and less adequate. The reasons include:

1) Complex User Roles: Static role-based systems are ineffective for real-time decision-making in a near real-time, rapid change in user roles and responsibilities, whether in a remote or hybrid work environment.
2) Scalability Issues: When organizations grow, centralized systems start becoming a daunting task to manage access to many devices, users, and associated applications.

©IJRASET: All Rights are Reserved

3) Privacy Concerns: GDPR and CCPA regulations are very strict with regard to personal data, and it constantly poses a challenge to make sure that the personal data is accessed correctly and not tampered with by any party.

B. *Federated Learning: A Decentralized Approach*

Federated Learning (FL) is a cutting-edge machine learning method for scaling up and preventing privacy attacks in distributed systems. Lastly, in FL, local models are trained by organizations or devices (called remote training parties) based on their own data and send results (e.g., model updates or gradients) to a central unit (called the aggregator). By aggregation process, the system can construct a consolidated model without sharing raw data among the participants. Its highly decentralized nature reduces risks to such centralized storage of the data, as in the case of a data breach or access to sensitive data taken by some unauthorized person. Additionally, it also boosts privacy since models can be trained on local data without revealing the data itself. Federated learning can also be utilized in the development of intelligent access control systems to support real-time threats by extracting collaborative insights and adapting to these threats from different organizations.

C. *The Role of Federated AI in Cybersecurity*

Given the case of security and access control, federated AI is a robust solution to federated learning along with AI techniques. This approach enables organizations to:

1) Enhance Threat Detection: Federated AI pools the insights from an array of different organizations to quickly and reliably detect and respond to growing cyber threats. Security is maintained and shared in a secure and decentralized manner while improving collective defence capabilities.
2) Dynamic Policy Enforcement: Once insights from the distributed data sources are known, the access control policies can be changed dynamically. With this, the system is more adaptive and can enforce more granular, context-sensitive access decisions.
3) Ensure Privacy Compliance: Federated AI systems can utilize privacy-preserving techniques, such as differential privacy and homomorphic encryption, to ensure user and organizational data is protected in accordance with global data protection regulations.

II. LITERATURE OVERVIEW

A. *Federated Learning for Cybersecurity Applications*

Federated Learning (FL) is a novel approach to cybersecurity, and its solutions are being applied to collaborative model training while preserving data privacy. In sensitive industry sectors like healthcare, finance, and (critical) infrastructure, privacy is sacrificed at the altar by centralized data sharing, and this is of special interest. FL makes threat detection much more powerful by enabling organizations to pool their insights and take advantage of collective intelligence. [5-8] As a case in point, a study illustrated that FL allows entities to detect and respond quickly to evolving cyber threats, gaining the benefit of knowledge from distributed datasets without revealing individual data records. The data confidentiality and proactive security measures are balanced under this paradigm, which makes the road for advanced collaborative intelligence in cybersecurity.

B. *Design of Federated Learning Systems*

Much attention has been paid to the development of FL systems for a given cybersecurity need. This paper takes an example of an FL-based system to demonstrate its deployment in HRM for security improvement. Collaborative model training is used to improve malware detection during the recruitment process by focusing on data privacy compliance with regulations such as GDPR. This example demonstrates that FL frameworks can flexibly adapt to domain-specific security challenges. Additionally, the rapid growth of FL systems calls for securing the privacy and security aspects while ensuring they fit into organizational goals, a premise that is crucial for increased acceptance.

C. *Access Control in Distributed Systems*

When integrating FL, access control is still a persistent challenge. Very often, dealing with the various decentralized access rights through traditional models is hard to manage. As a granular and dynamic policy enforcement solution, Attribute Based Access Control (ABAC) has gained the attention of large enterprises and developers. ABAC is used in FL systems, as it enables flexible access management by assigning rights depending upon the user attributes, including roles or behavioral patterns. Federated environments, where multiple stakeholders require varying levels of access to shared insights, rely on adaptability of this kind.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ABAC integration enriches security and compliance with privacy regulations by solving the two challenges of decentralized access control and data confidentiality.

D. Innovative Threat Detection Mechanisms

Previous applications of FL have expanded into developing innovative mechanisms for threat cybersecurity detections. For example, within FL frameworks, there is one notable advance that pertains to attention-based Graph Neural Networks (GNNs). However, these GNNs are collaborative analyses of network traffic patterns between organizations and identify anomalies attributed to potential intrusions. Preserving data privacy and decentralizing analysis enable this approach to be a more accurate Intrusion Detection System (IDS) with high data confidentiality. These are examples of how FL is transforming the real-time threat detection space by providing proactive responses to overcome sophisticated cyber-attacks.

III. METHODOLOGY

The Federated Learning (FL) process, a decentralized machine learning paradigm wherein multiple client devices collaborate to train a global model without sharing sensitive data, is illustrated by the diagram. Local model updates, Δw1, are performed by each device (labeled with icons representing various devices (e.g., tablet, car, phone, etc.) based on its own data. Then, these updates are sent back to the central FL Server, and it aggregates them to form a global model, as shown at the top of the image, using the mathematical formula. For k client devices (contribute nk/n to the model) each, local updates are aggregated through the process to a single aggregation node. [9] The beauty of this process is that individual devices like smartphones or IoT devices can calculate it as part of the model, and the raw data is not revealed. It's all for privacy and security. The global model is updated with validation results, aggregated and thus updated, and sent back to the client devices for additional iterations of training. The Federated Learning system consists of an iterative cycle of local updates and global aggregation to collaborate among distributed devices while preserving the privacy of sensitive data.

The implementation of access control in distributed systems is complex, authentication methods are inadequate, and there are scalability issues. [10-14] This Complexity of Implementation results from our requirement to design and enforce sophisticated access control policies for different user roles and deferential security requirements. In the absence of basic understanding and detailed planning, policies may not thwart risks sufficiently, resulting in systems being easy prey for unauthorized access. The second key challenge is Inadequate User Authentication. Unfortunately, for various reasons, many systems rely on over- or under-used authentication mechanisms that pose an increased risk of unauthorized access to critical resources. To handle this, we need robust authentication techniques, such as Multi-Factor Authentication (MFA), that extend beyond authentication with credentials. Scalability and Flexibility Issues make the deployment of access control fraught in growing organizations and, in this case, the last. Traditional models don't always support as user roles grow and expand, and this often requires access privileges to be changed frequently. Security requires that organizations follow the principle of least privilege and ensure that only users need the minimum amount of access to resources to do their jobs. Specific objectives that are proposed include forming a Federated Learning (FL) integrated framework, which will improve the adaptability and efficiency of access control policies while meeting privacy constraints and bolstering threat detection through collaborative intelligence.

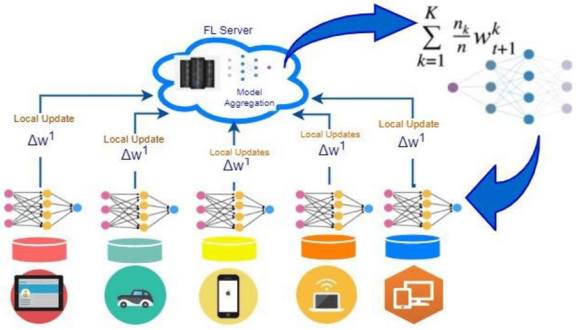


Figure. 1 Federated Learning Architecture

A. Federated Learning Framework

A Federated Learning (FL) framework typically comprises two main components:

1) Aggregator: An administrator-managed model fusion centralized unit. In this case, model updates (gradients) collected from remote nodes are aggregated by the aggregator to a single global model without using raw data.

2) Remote Training Parties: Independent training of local models on data with each distributed node or system. These are the nodes that periodically share their updates with the aggregator, allowing collaborative learning across the whole network.

FL is built on a cornerstone of Decentralized Data Processing; organizations can train models locally respecting data privacy. FL offers freedom from the consequent of sensitive information to ensure placement with privacy promises such as GDPR while boosting model precision through collective seeking. Another advantage of FL is Dynamic Policy Enforcement. With insights from the distributed data, the access control policies can be dynamically changed to support granular and context-aware decisions. This versatility ensures that access permissions stay in lockstep with current-day real-time business requirements, even in highly dynamic environments.

B. Security Enhancements

To ensure the security of a federated learning framework, it is essential to incorporate privacy-preserving techniques and robust defence mechanisms:

1) Privacy-Preserving Techniques: Data protection during the FL process is strongly supported by methods like differential privacy and homomorphic encryption. For instance, we use a distributed Paillier cryptographic mechanism such that local gradient information is still secure from inference attacks but can still facilitate collaborative training. These techniques provide good guarantees of confidentiality so that organizations can participate in federated learning without fear of any sensitive information leakage.
2) Defence Mechanisms against Adversarial Attacks: Poisoning attacks pose vulnerabilities to federated learning systems in that malignant actors attempt to alter corrupted data to paralyze model performance. RAB2-DEF is a defence mechanism that provides dynamic and explainable protection against such threats. These systems' defences for those attack scenarios are robust without jeopardizing the fairness and precision of the model. Moreover, federated frameworks can sustain high performance that is not violated by adversarial conditions by placing resilience at the top of the hierarchy.

C. Federated AI architecture for Cyber defence:

Architecture of the Federated AI system for cybersecurity illustrated the synergy between decentralized intelligence and robust security systems. It comprises three core components: Each one playing its role in Access Control, Federated AI System, and

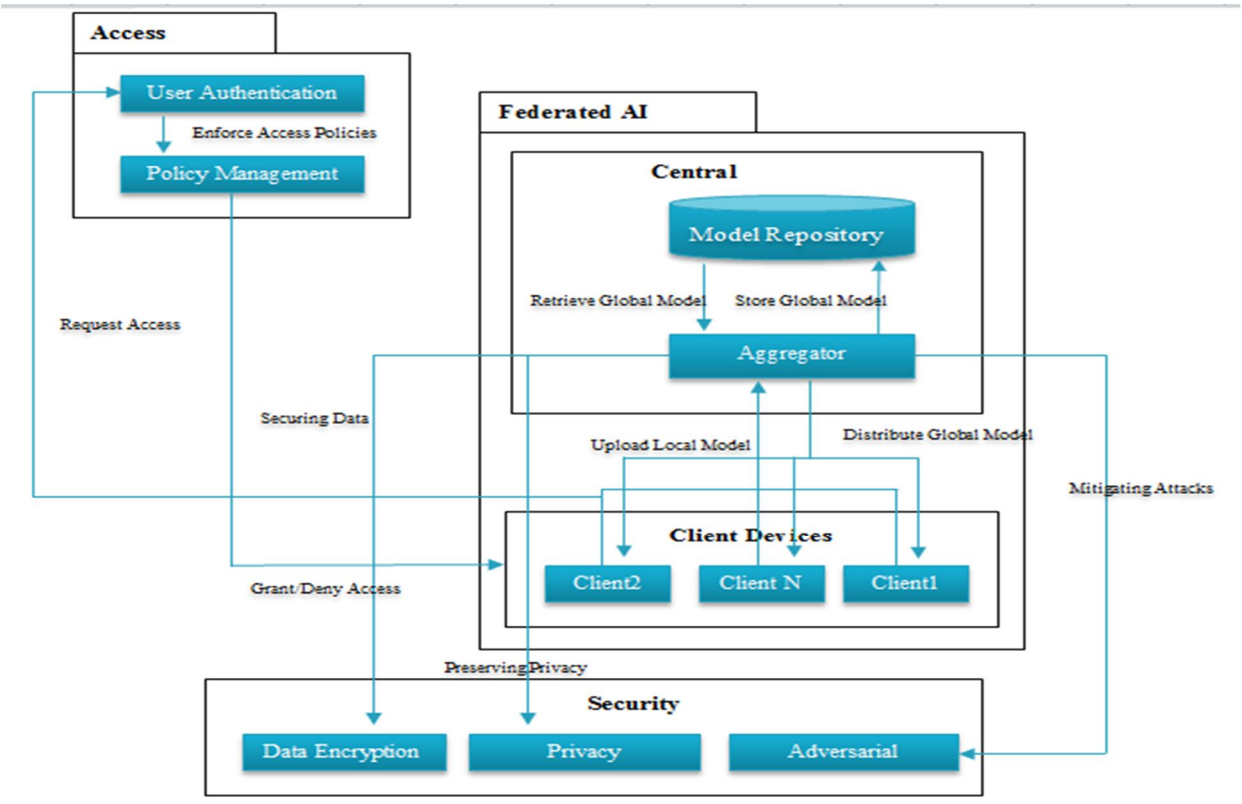


Figure 2: Federated AI Architecture for Cyber Defence

Security Mechanisms. Through such architecture, accessing controlled data in distributed environments becomes efficient in terms of access control, data privacy, and resiliency against adversarial attack threats. User authentication is done in the Access Control Module, which also enforces access policies and makes real-time decisions to grant or deny access. It talks to Federated AI systems and uses federated model insights to adapt policies on the fly. As a result, this capability improves accuracy and context-awareness in decision-making when managing access requests.

The Federated AI System anchors collaborative learning. Using encrypted updates shared to a centralized aggregator, models are trained locally to client devices (e.g., IoT devices, laptops) and then shared back to the aggregator. The aggregator creates these updates into a global model in a model repository on the central server. The global model is retrained further, thus continuously learning (but localization of the data, protecting user privacy). The Security Mechanisms layer complements this and implements encryption, privacy preserving, like differential privacy, and adversarial defences, such as RAB2-DEF. These measures protect sensitive data, secure communication, and protect the system against malicious attacks such as data poisoning or evasion attempts. This architecture is interconnected with scalable, privacy-preserving and resilient cybersecurity operations. It provides support for seamless collaboration among distributed nodes and centralized control and hence meets the ever-varying needs of such organizations, making it a vital framework for today's distributed systems

D. Implementation

The work here addresses the question of how one can implement the Federated AI system proposed to improve access control in distributed environments.

We then detail the system design, deployment architecture, dataset preparation, and the metrics used to evaluate the system. A new Federated AI system is designed using current state-of-the-art tools and technologies but chosen to take advantage of their specific role in constructing a secure and efficient framework. [15-18] The system features important components: an aggregator node, remote training nodes, communication protocols, and privacy-preserving techniques.

The aggregator node encodes model updates by remote training nodes and then aggregates them to a global model. To do this, TFF or PySyft tools allow this process while data stays secure. Local model training of decentralized datasets is performed at remote training nodes, including edge devices such as Raspberry Pi or laptops, so that sensitive data stays within the local environment. Protocols such as gRPC or MQTT are used to allow for secure communication between nodes and the aggregator. In federated learning systems, privacy and security are critical. Merging techniques such as Differentia Privacy and Homomorphic Encryption enable model training to maintain data confidentiality. Further, we utilize advanced tools such as Graph Neural Networks (GNNs) and anomaly detection libraries to facilitate collaborative network anomaly detection. The modular system architecture has been designed that integrates well with present cybersecurity tools and access control systems. Its scalability facilitates its ease of growth according to the organizational need, and the fact that it is a valid interoperable system means that the system is compatible with other devices and operating environments.

E. Deployment Architecture

The federated AI system deployment architecture describes the step-by-step integration of the system into already existing cybersecurity frameworks. It promotes the security of the system and the efficient implementation, with privacy maintained. First is installing the aggregator node so that it is a secure server (cloud or on-premises). The aggregator connects to remote training nodes that can be very far away over secure communication protocols such as gRPC or MQTT. We then define access control policies using Attribute Based Access Control (ABAC) to define rules for what a user role and attributes can have the rights to do. This is the stage where federated learning parameters like privacy thresholds or data-sharing constraints are initialized.

During the training phase, remote nodes train their models on their local datasets independently, and their gradient updates are encrypted and sent to the aggregator. Each update that the aggregation is provided generates a global model known by the nodes that can be refined back into the nodes. The process promotes locally sensitive data, reducing the probability of data breaches. Finally, the global model trained is deployed to the organization's access control system, making real-time decisions on what to deny access to, with updates to the model occurring in real-time to keep up with changes in the ecosystem and protect privacy. The deployment architecture is structured into four layers:

1) End-User Devices: System interaction starts with end-user devices. These devices will have client-side applications and contain local data required to train machine-learning models. Examples include the desktop, laptop or mobile device being used by the employees or system users. Data is processed decentralized, being able to interact with remote training nodes. This layer provides privacy and reduces data exposure risks by keeping all sensitive information locally.

2) Remote Training Nodes: Local training of machine learning models is performed with the help of remote training nodes. These nodes utilize the resources from edge devices (like Raspberry Pi, laptops, or on-premises servers) to train models on local datasets. The nodes receive a list of training steps for backward propaganda and use the sentences to send encrypted gradient updates to the aggregator node. The purpose of this layer is to maintain the decentralization of the raw data, which is part of the federated learning process. To allow our nodes to communicate efficiently and securely, we use the secure communication protocols gRPC or MQTT.

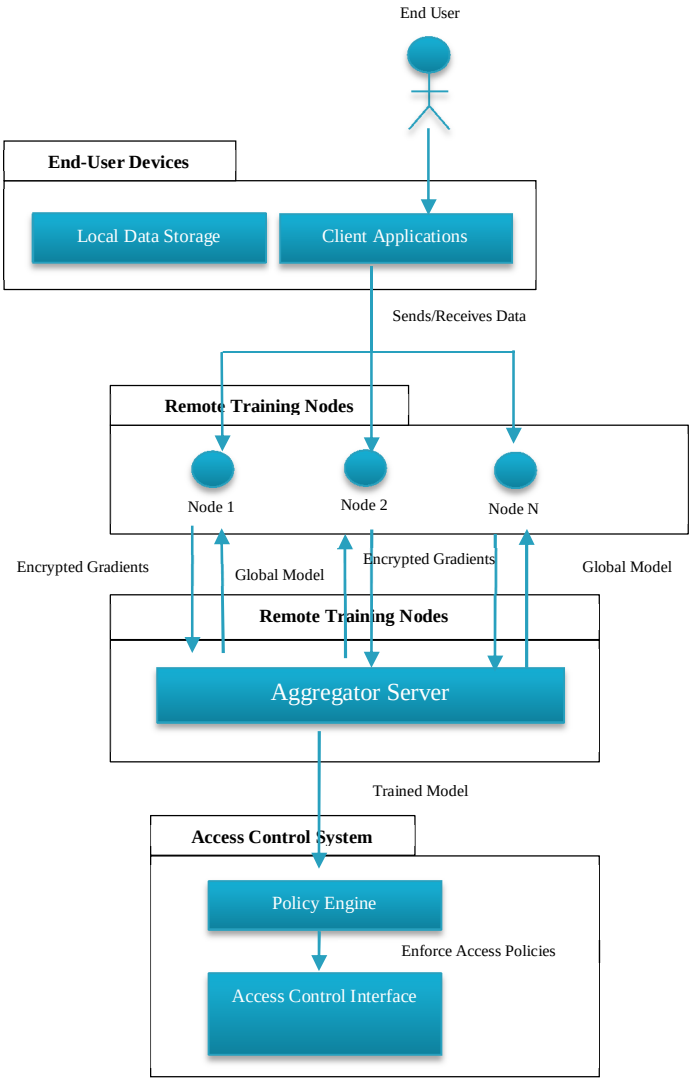


Figure 3: Deployment Architecture for Federated AI System

3) Aggregator Node: In federated learning, the aggregator node is the central coordination unit. The remote training nodes provide encrypted updates, which are then aggregated into a global model. Through this process, individual datasets are protected in privacy, yet this process enables collaborative intelligence. Then, the aggregator shares the global model to the nodes for more iteration. The aggregator node is hosted either on a secure cloud or on-premises servers; it ensures scalability, secure data handling and real-time coordination.

4) Access Control System: Finally, the access control system implements dynamic access control policies informed by federated learning insights. Components of such a system include a policy engine that evaluates user roles and attributes and an access control interface that uses policies in real-time. This layer integrates the outcomes of the federated model, providing granular resource access control and compliance with the organizational policies and regulatory frameworks.

F. Dataset and Preprocessing

According to researchers, the quality and preparation of datasets also determine the success of the Federated AI system. The framework is trained and evaluated with a combination of real-world and simulated datasets. For network intrusion detection, we use the UNSW-NB15 dataset from the University of New South Wales, and for detecting anomalies in network traffic, we employ the CICIDS2017 dataset from the Canadian Institute for Cybersecurity. Second, custom datasets collected from participating organizations offer access to and view behavioral patterns. A highly comprehensive preprocessing of the datasets is performed to ensure they are suitable for training. Data cleaning is about removing duplicates, incomplete entries or outliers. The dataset is normalized based on numerical features, and categorical features are provided as encoded values to ensure consistency. Automated tools, like FeatureTools, extract relevant features, such as user roles, resource access logs, and network traffic patterns. The datasets are then split into smaller subsets distributed across local nodes following realistic, decentralized data distributions. During preprocessing, preprocessing of gradients using Paillier Cryptosystem ensures data privacy and secure collaboration does not expose sensitive data.

G. Evaluation Metrics and Monitoring

The Federated AI system is evaluated using a set of metrics aimed at performance, privacy, and resource utilization. Some metrics to model accuracy measure how the system can make the correct access control decisions. Potential misclassification in anomaly detection is identified by calculating false positive and negative rates. Metrics such as privacy loss (ε) in differential privacy and compliance with data protection requirements are quantified for privacy. Communication overhead is also measured to resolve the amount of network bandwidth required during the process of training. Monitoring is done continuously as it's important to maintain system reliability. Anomalies are weathered, alerts are generated, and detailed logs are maintained for audit purposes. The benefit of this structured approach is that the system stays secure, adaptable, and efficient in scaling access control in distributed environments.

IV. RESULTS AND DISCUSSION

In this section, we experimentally evaluate Federated AI, focusing on the experimental design metrics and the results obtained. [19,20] Thus, it seeks to evaluate the system as a means for validating that the system maintains secure, scalable, and privacy-preserving access control in these distributed environments. Several critical metrics for the Federated AI framework's performance were assessed. The correctness of predictions by the federated model on enforcing access controls was evaluated by model accuracy. False Positive Rate (FPR) was the percent of legitimate actions that were mistakenly marked as unauthorized, and False Negative Rate (FNR) was measured as the percent of unauthorized actions that could not be identified as invalid. The system used Privacy Loss (ε), a quantification of data confidentiality based on differential privacy techniques, to secure robust privacy guarantees. We evaluated latency, the time required to update models and enforce policies, a key thing for real-time access control systems. We analyzed the communication overhead metric in federated training, showing how the framework controlled bandwidth usage. Finally, scalability was evaluated to investigate how well the system performed as the number of nodes participating increased. Together, these metrics served as one complete assessment of the system's effectiveness.

A. Experimental Setup

An experimental setup was developed to allow an emulation of a realistic deployment scenario for the Federated AI framework. Hardware included a powerful aggregator node running on an AWS EC2 instance with 16 vCPUs, 64GB RAM, and 1TB SSD storage. Raspberry Pi 4 devices with 4GB RAM and 128GB storage were used to simulate the remote training nodes. Giving TensorFlow Federated and PySyft as inputs and having Python as our core language of choice, we developed the framework. Secure protocols such as gRPC, HTTPS, etc were used to communicate nodes with each other.

Table 1: Hardware and Software Configuration

Component	Specification
Aggregator Node	AWS EC2 Instance (16 vCPUs, 64GB RAM, 1TB SSD)
Remote Training Nodes	Raspberry Pi 4 (4GB RAM, 128GB storage)
Development Framework	TensorFlow Federated, PySyft
Programming Languages	Python
Communication Protocols	gRPC, HTTPS

The experimental process was split into several phases. Using baseline testing, the concepts of a centralized machine learning model in terms of accuracy, latency, and privacy. The framework was tested using access control simulation, which simulated dynamic policy enforcement for legitimate and unauthorized access.

To evaluate resilience, adversarial techniques such as data poisoning and model evasion were used in attack simulations. Then scalability testing was performed, with the number of training nodes increasing incrementally to test system performance under varying loads. The experiments were similar to practical scenarios because they used partitioned real-world datasets such as UNSW-NB15 to mimic a distributed environment.

B. Results and Analysis

The results demonstrate that the Federated AI framework achieved competitive accuracy with centrally trained models. For example, centralized AI had an accuracy of 96.5 percent versus 95.2 per cent with federated AI without privacy measures. Differential privacy was incorporated so that the accuracy dropped slightly to 93.7%, showing that there is a trade-off between accuracy and privacy. Nevertheless, the improvement in data confidentiality made the trade-off acceptable.

Table 2: Accuracy vs. Privacy Trade-Off

Model Type	Accuracy (%)	Privacy Loss (ε)
Centralized AI	96.5	High
Federated AI (No Privacy)	95.2	Medium
Federated AI (Differential Privacy)	93.7	Low

1) Communication Overhead:

Bandwidth consumption was measured for different numbers of training nodes. Communication overhead was found to increase linearly with the number of nodes. For instance, the consumption of bandwidth was 120MB with 10 nodes, and it increased to 1200MB for 100 nodes. Latency increased from 20ms for 10 nodes and 85ms for 100 nodes. The results of these findings showed that the framework could manage network resources in a scalable, efficient manner.

2) Attack Resilience:

The system was shown to be highly resilient against adversarial attacks. The accuracy drops for random data poisoning attacks for the RAB2-DEF defence mechanism when dropped without it was 15%, and with RAB2-DEF, it was 5%. Similarly, with defence mechanism, the accuracy drop decreased from 25% to 8% for the targeted label-flipping attacks. This demonstrated how robust security institutions should be developed to counter adversarial threats.

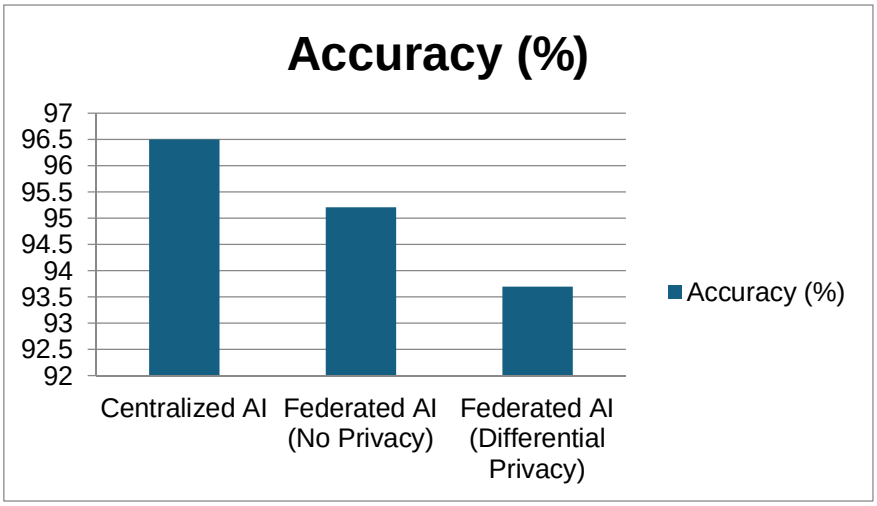


Figure 4: Graphical Representation of Accuracy vs. Privacy Trade-Off

Table 2: Bandwidth Consumption vs. Number of Nodes

Number of Nodes	Bandwidth Consumption (MB)	Latency (ms)
10	120	20
50	600	45
100	1200	85

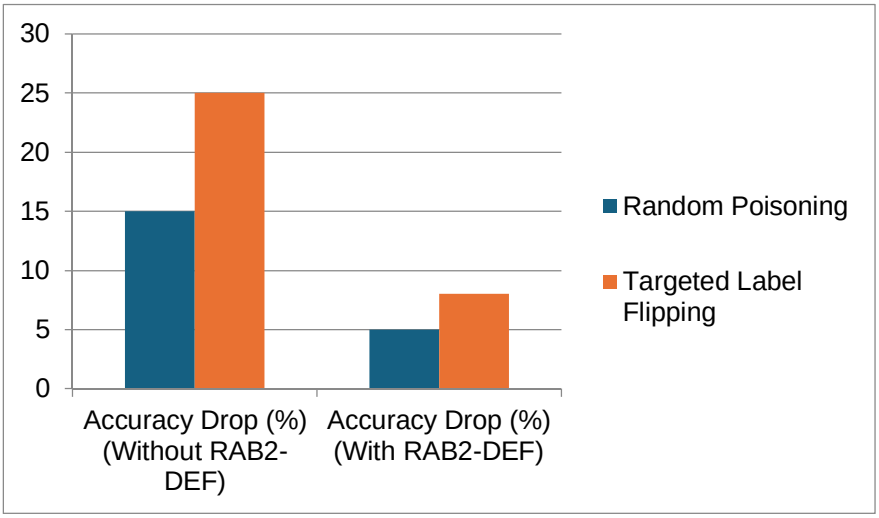


Figure 5: Graphical Representation of Accuracy Drop under Adversarial Attacks

3) Scalability Analysis

Its scalability was tested by running a different number of nodes. Training time also increased from 15 minutes when the number of nodes was 10 to 120 minutes when the nodes were 100. Despite that, model accuracy was very stable (decreasing only from 95% to 93%). It showed that the system was able to scale with minimal performance degradation.

Table 3: Accuracy Drop Under Adversarial Attacks

Attack Type	Accuracy Drop (%) (Without RAB2-DEF)	Accuracy Drop (%) (With RAB2-DEF)
Random Poisoning	15	5
Targeted Label Flipping	25	8

Table 4: Training Time vs. Number of Nodes

Number of Nodes	Training Time (Minutes)	Model Accuracy (%)
10	15	95
50	50	94
100	120	93

4) The privacy and performance trade-off

Differential privacy was used to show the effectiveness of privacy preserving techniques in experiments. We achieved an accuracy of 95.2% with privacy measures, but privacy loss was high. When combined with differential privacy with a ε value of 1.0, the accuracy slightly decreased to 93.7% while privacy loss was greatly reduced. It showed how the system reached equilibrium in terms of privacy and performance.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table 5: Privacy and Performance Trade-Off

Technique	Accuracy (%)	Privacy Loss (ε)
No Privacy Measures	95.2	High
Differential privacy (ε=1.0)	93.7	Low

In this section, the experimental results are critically evaluated, with merits and demerits of the Federated AI framework for distributed access control systems, and future directions for improvement of the Federated AI framework for use in distributed access control systems are suggested.

V. KEY FINDINGS

The federation AI framework's experimental evaluation showed that it helps to ensure better access control in distributed systems. The framework leveraged federated learning to dynamically respond to enforce access policies with competitive accuracy levels akin to centralized AI systems. It had a significant advantage in preserving data privacy, a concern about data protection and compliance with relevant regulations, e.g., GDPR. A notable output was the robustness of the system to adversarial attacks. RAB2-DEF advanced mechanisms helped the framework remain resilient to hostile environments as they continue to ensure the integrity of access control policies. At the same time, the framework could scale efficiently as the number of incoming nodes increased, but communication overhead grew linearly. Despite this expected growth, future techniques like compression or asynchronous updates can be used to optimize this in large deployments.

VI. LIMITATIONS

The framework, however, has some weaknesses which need to be rectified. A key limitation has to do with the accuracy vs privacy trade-off. By effectively protecting sensitive information, differential privacy slightly decreased a model's accuracy. For some applications that demand high precision, these factors may be balanced carefully, with privacy options decided on a need-to-need basis. The computational constraints of the edge devices, for example, the IoT node, result in another limitation. The federated learning process is often carried out on these devices that are missing the required processing power for more complex model training, resulting in inconsistent contributions to the learning process. Such imbalance can make the overall model performance degenerate and thus often needs to integrate lightweight training algorithms hardware optimizations. In addition, policy enforcement latency remains a concern as it is needed for much of the decision making to be made in a timely manner. When delays are possible due to updates, synchronization over time takes, and delays may impact the system's responsiveness. In addition, while the framework can tolerate certain adversarial attacks, existing adversarial attacks that target aggregation or communication protocols remain ongoing challenges that require additional development of robust defences.

VII. CONCLUSION

In this work, we extend access control in distributed systems using a Federated AI framework built on federated learning. The framework can support the collaborative model training mechanism across organizations, which ensures data privacy based on privacy regulations such as GDPR. With experimental evaluation, the framework showed significant improvements in access control through dynamic context-aware decision-making, robust privacy preservation and robustness to adversarial attacks. Furthermore, its ability to scale effectively across distributed environments makes it ideal for use widely. That proves Federated AI is a transformative approach to collaboration, privacy-preserving technologies and enhanced security measures. By addressing current issues of distributed access control, the framework lays the groundwork for developing secure, efficient, scalable solutions that are fundamentally important in creating a framework for secure future facilities in various organizational settings.

VIII. FUTURE WORK

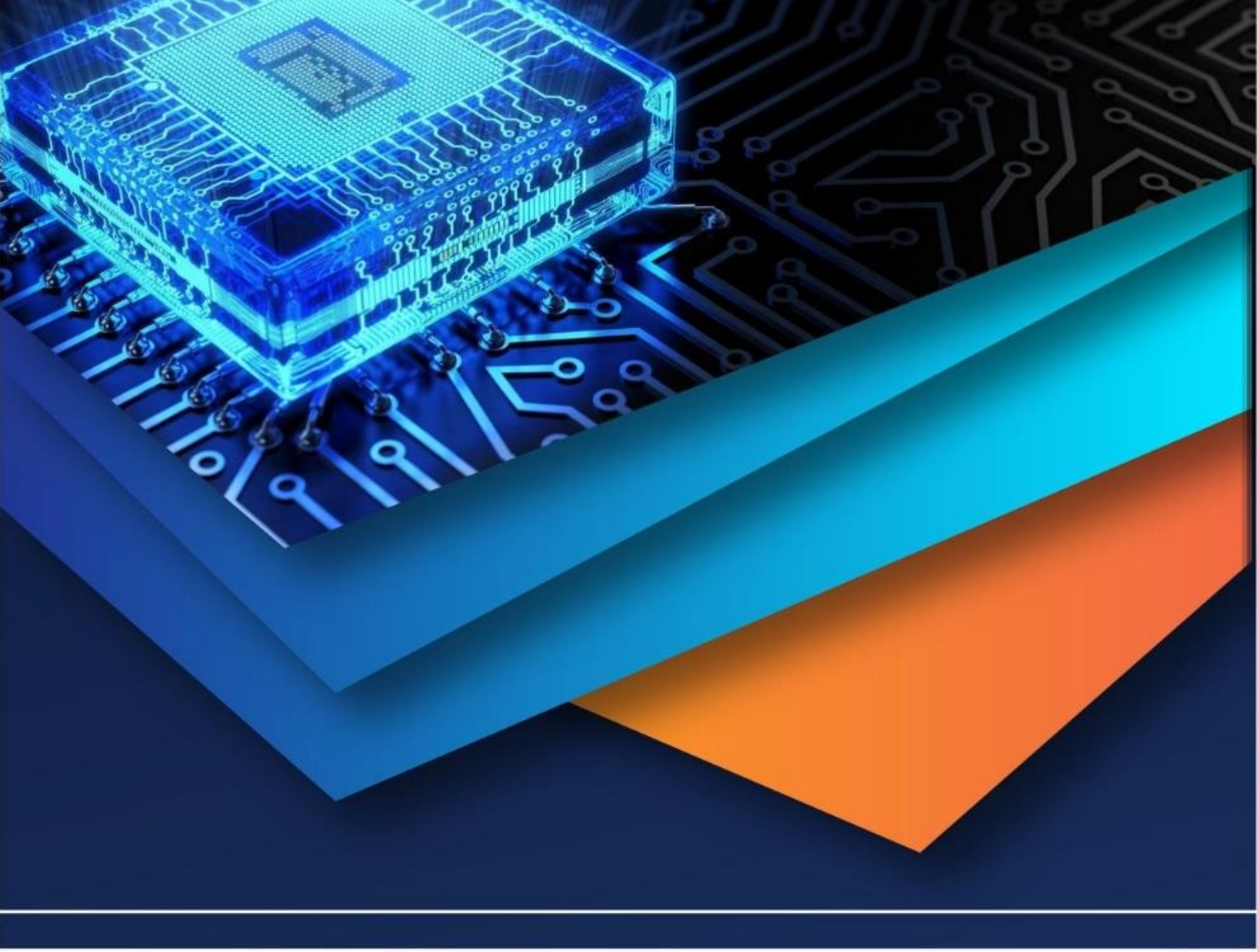
Despite the framework's good performance, there are many areas to improve. Still, advanced privacy techniques, including Secure Multi-Party Computation (SMPC) and federated distillation, can be considered to achieve a better trade-off between privacy preservation and model accuracy. Finally, communication protocols can also be optimized through model compression and asynchronous updates to lower latency and communications overhead, making the system even more efficient for large-scale deployments. Future research must also adapt the framework to resource-constrained environments such as IoT devices using lightweight models and edge-optimized algorithms.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Additional proof of its versatility would come from expanding its applicability to real-time systems, emerging domains such as smart cities, and advanced threat detection scenarios. Secondly, integrating robustness under adversarial settings and designing governance protocols will be important to make Federated AI reliable, ethical in use, and adopted in the long term by many industries.

REFERENCES

[1] Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet of Things Journal, 9(11), 8229-8249.
[2] Cuppens, F., Cuppens-Boulahia, N., & Ghorbel, M. B. (2007). High level conflict management strategies in advanced access control models. Electronic Notes in Theoretical Computer Science, 186, 3-26.
[3] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of things, 1(1), 7.
[4] Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. IEEE Access, 9, 138509-138542.
[5] Verlande, L., Lechner, U., & Rudel, S. (2022, November). Design of a Federated Learning System for IT Security: Towards Secure Human Resource Management. In Proceedings of the 11th Latin-American Symposium on Dependable Computing (pp. 131-136).
[6] Charlie Isaksson, Federated Learning for Cyber Security: What You Need to Know in 2021, phData, online. https://www.phdata.io/blog/federated-learning-for-cyber-security/
[7] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2018). Access control for emerging distributed systems. Computer, 51(10), 100-103.
[8] Federated Learning for Cybersecurity: Collaborative Intelligence for Threat Detection, Tripwire, 2024. online. https://www.tripwire.com/state-of-security/federated-learning-cybersecurity-collaborative-intelligence-threat-detection
[9] Shaheen, M., Farooq, M. S., Umer, T., & Kim, B. S. (2022). Applications of federated learning; taxonomy, challenges, and research trends. Electronics, 11(4), 670. – Image
[10] Jianping, W., Guangqiu, Q., Chunming, W., Weiwei, J., & Jiahe, J. (2024). Federated learning for network attack detection using attention-based graph neural networks. Scientific Reports, 14(1), 19088.
[11] Delinea Team, Access Control: Models and Methods, Delinea, online. https://delinea.com/blog/access-control-models-methods
[12] Shubhangi Srivastava, AI in Cybersecurity - Uses, Threats & Prevention, Engati, 2024. online. https://www.engati.com/blog/ai-in-cybersecurity
[13] Alazab, M., RM, S. P., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R., & Pham, Q. V. (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. IEEE Transactions on Industrial Informatics, 18(5), 3501-3509.
[14] Gavin Wright, What is access control?, Techtarget, online. https://www.techtarget.com/searchsecurity/definition/access-control
[15] Protecting AI with Federated Learning and Privacy-Enhancing Technologies, Scaleoutsystems, online. https://www.scaleoutsystems.com/ai-security-privacy
[16] Zhu, H., Zhang, H., & Jin, Y. (2021). From federated learning to federated neural architecture search: a survey. Complex & Intelligent Systems, 7(2), 639-657.
[17] Lo, S. K., Lu, Q., Zhu, L., Paik, H. Y., Xu, X., & Wang, C. (2022). Architectural patterns for the design of federated learning systems. Journal of Systems and Software, 191, 111357.
[18] John, M. M., Olsson, H. H., & Bosch, J. (2020, December). Ai deployment architecture: Multi-case study for key factor identification. In 2020 27th Asia-Pacific Software Engineering Conference (APSEC) (pp. 395-404). IEEE.
[19] Gu, X., Tianqing, Z., Li, J., Zhang, T., Ren, W., & Choo, K. K. R. (2022). Privacy, accuracy, and model fairness trade-offs in federated learning. Computers & Security, 122, 102907.
[20] Kumar, K. N., Mohan, C. K., & Cenkeramaddi, L. R. (2023). The impact of adversarial attacks on federated learning: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 46(5), 2672-2691.
[21] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Bioacoustic Signatures - Revolutionizing User Authentication in the Digital Age." International Journal of Innovative Research in Science, Engineering and Technology, vol. 13, no. 12, 9, Dec. 2024, www.ijirset.com/upload/2024/december/9_Bioacoustic.pdf.
[22] Sreejith Sreekandan Nair, Govindarajan Lakshmikanthan."Enhancing the Resilience of Cloud-Based Security Solutions: Lessons from CrowdStrike Outage", Volume 12, Issue XII, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 915-926, ISSN : 2321-9653, www.ijraset.com
[23] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Global Fortification - Unifying Global DDoS Defense." International Journal of Innovative Research in Computer and Communication Engineering, vol. 11, no. 6, 81, June 2023, ijircce.com/admin/main/storage/app/pdf/nM8AGEVjgzqWgfqkH8vMHkTs3HJ32PLhXaG4mDpO.pdf.
[24] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Proactive Cybersecurity: Predictive Analytics and Machine Learning for Identity and Threat Management." International Journal of Innovative Research in Computer and Communication Engineering, vol. 12, no. 12, Dec. 2024, ijircce.com/admin/main/storage/app/pdf/qyDA9xUcvRKOpzstDBJRrZfv1amr8WIhUcOFFhQg.pdf.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)