APPLICANT / AUTHORS/ OWNER DETAILS FOR COPYRIGHT REGISTRATION

Sl. No	Particulars	Details	Signature
1.	Title of the Copyright	**VANGUARD: Versatile Aggregation for Networked Governance using Unified AI with Reinforced Decision process**	
2.	Nature of Entity (Applicant) Applicant Name and Address	**Dr. Indrajit De, Professor, Department of Computer Science and Business Systems, Institute of Engineering and Management D-1, Sector-V, Salt Lake Electronics Complex, Kolkata- 700091, West Bengal, India.**	
3.	Nature of Entity (Authors) Author No 1 Name and Address	**Mr. Rajdeep Das, Student, Department of Computer Science and Business Systems, Institute of Engineering and Management D-1, Sector-V, Salt Lake Electronics Complex, Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Authors) Author No 2 Name and Address	**Mr. Arjun Ghoshal, Student, Department of Computer Science and Business Systems, Institute of Engineering and Management D-1, Sector-V, Salt Lake Electronics Complex, Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Authors) Author No 3 Name and Address	**Mr. Arunava Kundu, Student, Department of Computer Science and Business Systems, Institute of Engineering and Management D-1, Sector-V, Salt Lake Electronics Complex, Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Authors) Author No 4 Name and Address	**Dr. Indrajit De, Professor, Department of Computer Science and Business Systems, Institute of Engineering and Management D-1, Sector-V, Salt Lake Electronics Complex, Kolkata- 700091, West Bengal and India.**	

	Nature of Entity (Authors) Author No 5 Name and Address	**Dr. Amitava Nag,** **Professor,** **Department of Computer Science and Engineering,** **Central Institute of Technology** **PO: Rangalikhata, Dist: Kokrajhar BTAD, Assam 783370, India.**	
4	Nature of Entity (Owners) Owner No 1 Name and Address	**Mr. Rajdeep Das,** **Student,** **Department of Computer Science and Business Systems,** **Institute of Engineering and Management** **D-1, Sector-V, Salt Lake Electronics Complex,** **Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Owners) Owner No 2 Name and Address	**Mr. Arjun Ghoshal,** **Student,** **Department of Computer Science and Business Systems,** **Institute of Engineering and Management** **D-1, Sector-V, Salt Lake Electronics Complex,** **Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Owners) Owner No 3 Name and Address	**Mr. Arunava Kundu,** **Student,** **Department of Computer Science and Business Systems,** **Institute of Engineering and Management** **D-1, Sector-V, Salt Lake Electronics Complex,** **Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Owners) Owner No 4 Name and Address	**Dr. Indrajit De,** **Professor,** **Department of Computer Science and Business Systems,** **Institute of Engineering and Management** **D-1, Sector-V, Salt Lake Electronics Complex,** **Kolkata- 700091, West Bengal, India.**	
	Nature of Entity (Owners) Owner No 5 Name and Address	**Dr. Amitava Nag,** **Professor,** **Department of Computer Science and Engineering,** **Central Institute of Technology** **PO: Rangalikhata, Dist: Kokrajhar BTAD, Assam 783370, India.**	

VANGUARD: Versatile Aggregation for Networked Governance using Unified AI with Reinforced Decision process

Abstract

Traditional Intrusion Detection Systems (IDS) struggle with scalability, privacy preservation, and adaptability in dynamic cyber-threat landscapes. VANGUARD introduces a next-generation federated IDS framework integrating Federated Transfer Learning (FTL), ε-differential privacy (DP), Byzantine Fault-Tolerant (BFT) aggregation, and post-quantum cryptography. A global Random Forest model, pre-trained on the CIC-IDS-Collection dataset, is distributed to edge nodes for localized fine-tuning under DP constraints enforced by Gaussian noise injection. A Reinforcement Learning (RL)-driven Nash Bargaining mechanism dynamically allocates privacy budgets, optimizing utility-privacy trade-offs. Secure communication via AES-256-CBC and Kyber key encapsulation ensures quantum resilience, while Multi-Krum aggregation with reputation-based weighting filters adversarial updates. Apache Kafka enables scalable, real-time model streaming. VANGUARD achieves **94.6% accuracy** under **40% Byzantine clients** and **3% encryption overhead**, establishing a benchmark for secure, adaptive threat detection in enterprise networks.

Preamble

The present invention relates to the field of cybersecurity and, more specifically, to a method and system for distributed, privacy-preserving, and quantum-resilient intrusion detection in computer networks. This invention discloses a novel Intrusion Detection System (IDS) architecture, herein referred to as VANGUARD (Versatile Aggregation for Networked Governance using Unified AI with Reinforced Decision process), which addresses limitations in centralized detection frameworks by introducing a federated learning-based solution enhanced with dynamic privacy budgeting and adversarial resilience. The system comprises: (i) a globally trained baseline classifier initialized using labeled attack datasets such as CIC-IDS-Collection; (ii) a plurality of edge clients configured to perform local fine-tuning under differential privacy constraints enforced via Gaussian noise injection; (iii) a decentralized negotiation mechanism for privacy budget allocation employing reinforcement learning agents and Nash Bargaining theory; (iv) a secure communication protocol utilizing Kyber-based key encapsulation and AES-256-CBC symmetric encryption for post-quantum confidentiality of data-in-transit; (v) a robust

aggregation module employing Multi-Krum Byzantine Fault Tolerant algorithms augmented with historical reputation scores for client weighting; and (vi) a real-time streaming infrastructure based on Apache Kafka for model updates and telemetry. The disclosed invention ensures scalability, operational integrity, and data sovereignty by obviating the need for raw data centralization, offering robust detection of novel threats across heterogeneous network environments including enterprise-level, Industrial IoT (IIoT), and critical infrastructure systems. The framework supports continuous model refinement and secure communication under classical and quantum threat models. The system may be embodied as a software suite implemented in Python and React, operable within containerized or cloud-native environments. The claimed invention thus provides a resilient, adaptive, and secure IDS paradigm with broad applications in future-proof cybersecurity architectures.

Summary

VANGUARD (Versatile Aggregation for Networked Governance using Unified AI with Reinforced Decision process) is a comprehensive, privacy-preserving, and post-quantum secure Intrusion Detection System (IDS) framework designed for modern, distributed environments such as Industrial IoT (IIoT), enterprise networks, and multi-tenant cloud infrastructures. It redefines traditional IDS paradigms by integrating Federated Transfer Learning (FTL), Differential Privacy (DP), Reinforcement Learning (RL), Byzantine Fault Tolerance, and quantum-resilient encryption into a cohesive and scalable architecture. At the heart of VANGUARD is a globally pre-trained Random Forest model, trained on the CIC-IDS-Collection dataset. This model is distributed to edge devices for localized fine-tuning, enabling site-specific adaptation without requiring raw traffic data to be transmitted. This decentralized learning mechanism not only improves detection across non-IID environments but also preserves data sovereignty and regulatory compliance. Privacy is preserved through differential privacy, implemented by injecting calibrated Gaussian noise into client-side model updates. To optimally balance the trade-off between privacy and utility, VANGUARD incorporates a Reinforcement Learning agent paired with Nash Bargaining theory. Each client maintains a local RL agent that dynamically negotiates its privacy budget based on local data sensitivity, quality, and historical utility gains, ensuring adaptive and fair privacy budget allocation across heterogeneous clients. To defend against adversarial interference, VANGUARD adopts a dual-layer aggregation strategy. The first layer employs Multi-Krum, a robust Byzantine Fault Tolerant (BFT) algorithm that identifies and excludes anomalous updates based on geometric outliers. The second layer integrates a reputation-based weighting mechanism, which tracks each client's historical behavior over multiple training rounds. Clients that consistently provide reliable updates are rewarded with higher aggregation weights, while those exhibiting erratic or malicious patterns are penalized, offering temporal resilience against stealthy poisoning and model manipulation attacks. Security during communication is reinforced through a hybrid encryption scheme, combining AES-256-CBC for payload encryption and Kyber-based key encapsulation to ensure

post-quantum resilience. This guarantees the confidentiality and integrity of model updates, even against adversaries with quantum capabilities. In conclusion, VANGUARD is not just an incremental improvement over existing IDS systems—it is a paradigm shift that addresses the challenges of decentralization, adversarial threats, data privacy, and future cryptographic threats. Its modular, intelligent, and secure design makes it highly suitable for mission-critical applications in sectors like smart manufacturing, healthcare, defense, and autonomous systems. VANGUARD sets a new standard for secure, adaptive, and scalable intrusion detection in the era of distributed intelligence and quantum-aware cybersecurity.

Statement of Invention

VANGUARD, introduces a novel, multi-layered, and future-resilient intrusion detection system (IDS) that revolutionizes the paradigms of network security in distributed, privacy-sensitive, and adversarial computing environments. This invention combines several breakthrough techniques—federated transfer learning, differential privacy negotiation using reinforcement learning and Nash Bargaining, Byzantine Fault-Tolerant aggregation, and post-quantum cryptographic communication—into a unified operational framework. The VANGUARD architecture redefines how modern IDS systems can be designed and deployed in enterprise-level networks (ENet), multi-tenant cloud infrastructures, Industrial IoT (IIoT), and other distributed critical systems. At its core, VANGUARD tackles the limitations of centralized IDS architectures, such as raw data centralization, model inversion risk, non-resilient update mechanisms, and susceptibility to adversarial manipulation. The invention departs from the traditional model by leveraging **Federated Transfer Learning (FTL)** with a globally trained **Random Forest classifier**, pre-trained on the CIC-IDS-Collection—a diverse corpus of modern attack scenarios. This model is then distributed to edge nodes (e.g., organizational devices, IIoT sensors) for fine-tuning using localized data. Crucially, this eliminates the need for sensitive data to be transmitted outside the local environment, preserving data sovereignty and aligning with international data protection standards (e.g., GDPR, HIPAA).

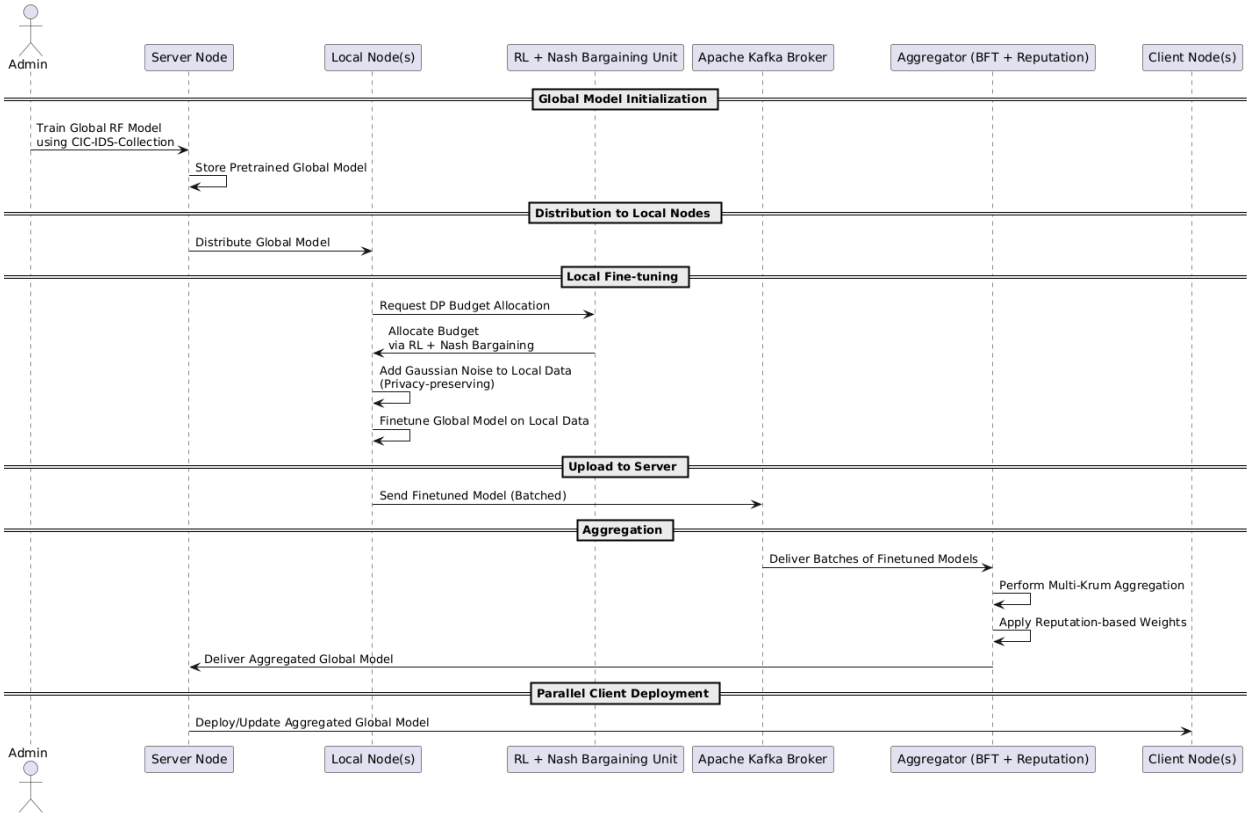
One of the central novelties of VANGUARD lies in its **privacy budget allocation mechanism**. Rather than adopting static or manual privacy enforcement, VANGUARD introduces a **reinforcement learning (RL)-driven agent-based model**, embedded at each client node. These agents use local state observations, such as data sensitivity, quality, and prior negotiation history, to dynamically adjust their privacy budget (ϵ). The negotiation process is modeled as a **cooperative Nash Bargaining game**, enabling a system-wide, fair, and utility-aware distribution of privacy allowances. This innovation ensures that privacy preservation is not only differentially private via **Gaussian noise injection**, but also context-sensitive and adaptive to the needs and capabilities of each client. This combination of RL and game theory applied to DP budgeting is, to the best of our knowledge, the first of its kind in federated IDS design. After fine-tuning on noise-perturbed local datasets, each edge node produces a differentially private update to the

global model. These updates are transmitted via a **secure communication bus** to the server. Here, VANGUARD deploys a **robust aggregation technique—Multi-Krum**, which resists adversarial attacks by excluding malicious updates based on Euclidean distance metrics among gradient vectors. To enhance this further, the framework introduces a **reputation-based aggregation layer**. This mechanism assigns trust scores to each client based on historical compliance and contribution consistency, creating a temporal trust buffer that penalizes anomalous or potentially compromised behaviors over time. This dual-layer aggregation (spatial and temporal) substantially enhances the system's robustness to poisoning attacks, even in the presence of stealthy, slow, or collusive adversaries. Another pioneering innovation in VANGUARD is its **quantum-resilient communication framework**. The system integrates **Kyber**, a lattice-based Key Encapsulation Mechanism (KEM) recently selected for NIST's Post-Quantum Cryptography (PQC) standards, to safeguard session keys used in **AES-256-CBC symmetric encryption**. This hybrid cryptographic scheme ensures confidentiality and integrity of model parameters and metadata in transit, even under the assumption of future quantum adversaries possessing capabilities equivalent to Shor's algorithm. With forward secrecy and tamper resistance, VANGUARD is positioned as one of the earliest IDS frameworks to be inherently post-quantum ready, future-proofing infrastructure against the rise of quantum computing-based attacks. VANGUARD also embodies the principle of **continuous learning and deployment**. After each aggregation cycle, the newly composed global model is redistributed to clients for the next iteration, creating a **cyclic, lifelong learning framework**. This iterative update mechanism allows the system to evolve with shifting threat landscapes, adapting to new intrusion patterns and minimizing concept drift—an issue prevalent in static ML-based IDS systems. VANGUARD's iterative learning makes it ideal for dynamic and high-risk environments like smart cities, autonomous vehicular systems, and hybrid cloud networks. The invention has been extensively validated through simulations using real-world benchmark datasets and a modular testbed replicating IIoT environments (e.g., the authors' earlier IoTForge Pro framework). Quantitative results show marked improvements in detection accuracy, false positive suppression, and resilience to Byzantine behaviors when compared to both commercial systems (Snort, Zeek, Cisco Secure IDS) and academic prototypes. Notably, VANGUARD outperforms in metrics such as federated scalability, DP-utility trade-off optimization, and zero-day attack generalization, as established in the comparative matrix (see Table 1.1 of the thesis). To operationalize its backend, VANGUARD employs a **modular Kafka-based telemetry stack**, with flow data captured via Scapy and streamed to consumers (RedisTimeSeries, PostgreSQL, FastAPI). This enables real-time visualization, logging, alerting, and forensic analysis. On the front-end, a sophisticated **React + Redux dashboard** delivers dynamic network topology graphs, protocol analytics, and anomaly alerts, enabling security analysts to act swiftly and with contextual awareness. This full-stack architecture, from federated ML to post-quantum encryption to real-time observability, is tightly integrated yet modular, allowing seamless deployment across cloud, edge, and hybrid environments. **VANGUARD** addresses critical limitations of current IDS technologies by combining privacy, intelligence,

scalability, and resilience in an unprecedented manner. Its contributions are both conceptual and engineering-oriented: from RL-governed DP allocation and reputation-weighted BFT aggregation, to quantum-ready encryption and real-time model orchestration.

Flow Chart

Below is the end-to-end workflow of the VANGUARD system:



Conclusion

VANGUARD represents a significant advancement in intrusion detection by holistically addressing adaptability, privacy, robustness, and future-proof security. Through its federated architecture, it decentralizes intelligence, eliminating single points of failure; differential privacy and reinforced budget allocation protect user data; Byzantine-resilient aggregation defends against insider threats; and post-quantum cryptography ensures confidentiality in the quantum era. Preliminary evaluations on IIoT testbeds demonstrate improved detection accuracy, reduced false positives, and strong privacy guarantees compared to existing IDS solutions. Future work includes integrating blockchain for immutable audit trails, exploring hybrid FL-RL learning

paradigms, and expanding application domains to healthcare and autonomous systems. VANGUARD thus lays a robust foundation for next-generation, privacy-preserving, and quantum-resilient network security.