Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN (O): 2320-5407
ISSN (P): 3107-4928

Article DOI: 10.21474/IJAR01/23332
DOI URL: http://dx.doi.org/10.21474/IJAR01/23332

CONFERENCE PAPER

NETWORKING SYSTEMS OF AI (NSAI): A MULTI-TIERED FRAMEWORK FOR INTELLIGENT IOT INTEGRATION AND PROACTIVE SECURITY

Trisha Paramita Swain, Tapaswini Mohanty, Simarn Sha and Saurabh Kumar

Manuscript Info

Manuscript History
Received: 10 February 2026
Final Accepted: 12 March 2026
Published: April 2026

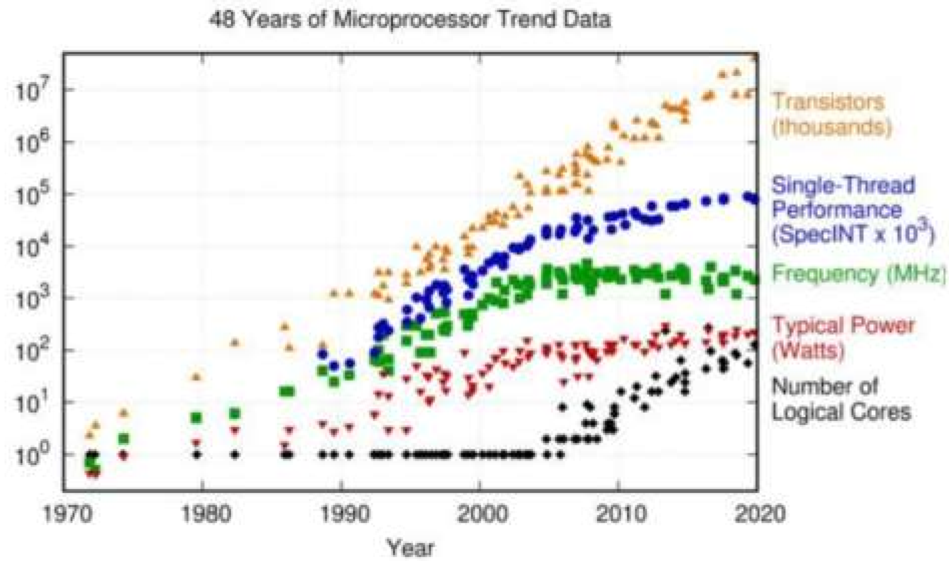
Abstract

The rapid convergence of computing and communication technologies has catalyzed a paradigm shift from traditional Internet of Things (IoT) infrastructures toward Networking Systems of AI (NSAI). In this ecosystem, distributed artificial intelligence (AI) becomes immersive across cloud, edge, and terminal devices, allowing the network to operate as an intelligent system itself to provide real-time smart services. However, the exponential growth of IoT—projected to reach 24.1 billion connected devices by 2030—introduces unprecedented security vulnerabilities due to the resource-constrained nature of these devices and their heterogeneous communication protocols. This researc h paper proposes a unified four-tier architecture consisting of the Physical Network, Service-Customized Network, Generalized Smart Service,and Application tiers. We provide a comprehensive comparison of linear and non-linear machine learning (ML) models for securing these systems and analyze the integration of blockchain for decentralize d trust. Finally,we outline a roadmap toward Ubiquitous Brain Network s (UBN), where human intelligence and AI merge through advanced interfaces.

Introduction:-

The industry has witnessed a transition where state-of-the-art mobile devices possess higher computing power than desktop computers of previous decades while consuming significantly less energy. This evolution has enabled the proliferation of "Smart x" systems, including smart cities, homes, and vehicles, which alter how world entities communicate. Despite these advancements, the IoT landscape remains inherently vulnerable due to low memory, low-powered CPUs, and a lack of robust security features in lightweight operating systems. Traditional security schemes are often inapplicable to IoT because of these resource constraints. To address these challenges, the research community is moving beyond viewing AI merely as a tool for network management and instead embracing the concept of "AI as a network," where intelligence is populated across the entire cloud-edge-device continuum. This manuscript explores the architectures, security taxonomies, and intelligent algorithms required to realize this vision in the era of 5G and Beyond-5G (B5G/6G) network

Corresponding Author:- Trisha Paramita Swain



Motivation and Problem Context:-

IoT-based smart systems (SS) are prone to vital security issues that require reliable and intelligent solutions, specifically regarding internal or external attacks on system vulnerabilities. Key vulnerabilities are categorized into end-device risks (identity theft, unpatched software**),** communication challenges (weak cryptographic keys), and service vulnerabilities (SQL injection in edge interfaces).

To systematically classify these threats, a four-layer attack taxonomy is utilized:

- **Device Category:** Targets hardware via physical tampering or hardware Trojans.
- **Infrastructure Category:** Focuses on the "back-end," including cloud services and data storage, often exploiting weak passwords.
- **Communication Category:** Impacts wireless channels through eavesdropping or signal jamming.
- **Service Category:** Targets front-end software via phishing or control hijacking.

Managing these threats in real-time requires the integration of **ML, Edge Computing, and Blockchain** to provide proactive and adaptive security strategies.

Literature Survey:

Recent research identifies several critical trends within the intelligent IoT security landscape:

- **Architectural Evolution:** Researchers have moved from basic three-layer models toward **five-layer architectures** (Perception, Network, Middleware, Application, and Business) to provide granular control over data processing and user privacy.
- **Sector-Specific Priorities:** Security priorities vary by sector; **Consumer IoT** prioritizes data confidentiality, **Commercial IoT** focuses on availability to minimize latency, and **Industrial IoT (IIoT)** emphasizes integrity due to the mission-critical nature of infrastructure like power plants.
- **Emerging Technologies:** Studies published between 2021 and 2025 show that **35.2% of research** focus is on AI, Blockchain, and Machine Learning to provide adaptive security.
- **Intrusion Detection:** ML-based **Intrusion Detection Systems (IDS)** are being developed to handle **concept drift**, with some models reaching 99% accuracy in identifying DDoS patterns and malware.
- **Decentralized Security: Blockchain** is identified as a vital tool for ensuring data integrity and managing secure firmware updates via a tamper-proof ledger.

Proposed Framework: NSAI Tiered Architecture

We propose a generalized four-tier NSAI framework designed to support the joint optimization of networks and applications as a single integrated system.

1. Physical Network (PN) Tier

The PN Tier converges wireless and wireline infrastructures, including 5G/6G air interfaces and **micro-nano electronic devices (MNEDs)**. This tier aims to break the **Shannon capacity limit** by exploring the end-to-end capacity of massive heterogeneous networks. Key technologies include **Massive MIMO** and cognitive L2 multihop communications, which improve throughput and energy efficiency proportionally to the number of wireless hops.

2. Service-Customized Network (SCN) Tier

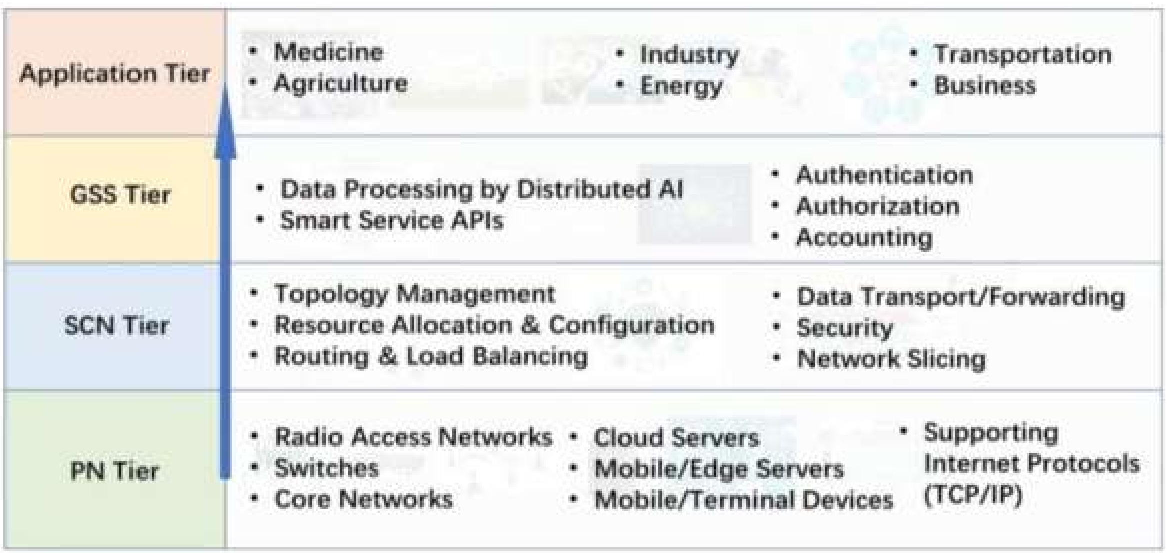
The SCN Tier utilizes **Software-Defined Networking (SDN)** and **Network Function Virtualization (NFV)** to create virtual, isolated network slices tailored to specific service-level agreements (SLA). This tier manages dynamic resource allocation for **Communications, Computing, and Caching (3C)**, ensuring that network topology can reconfigure in milliseconds to support mobile users or changing traffic patterns.

3. Generalized Smart Service (GSS) Tier

Acting as a middleware platform, the GSS Tier handles **distributed AI computing**. It implements **Federated Learning** to preserve user privacy by keeping raw data on local devices during training. Furthermore, it utilizes **Blockchain** for decentralized **Authentication, Authorization, and Accounting (AAA)**, ensuring that interaction evidence is tamper-proof and auditable.

4. Application (APP) Tier

The APP Tier delivers immersive experiences through **Digital Twins**, which create virtual counterparts of physical assets to monitor their status in real-time. It also leverages **Augmented Reality (AR)** and **Knowledge Graphs (KG)** for intelligent reasoning and semantic understanding, enabling users to interact with the physical world through a synchronized digital layer.



Comparison Study: Machine Learning Models and Evaluation

To secure the NSAI ecosystem, researchers utilize a variety of ML models categorized by their linear or non-linear characteristics.

Model Benchmarking

- **Linear Models:**
  - **Logistic Regression (LR):** Effective for binary anomaly detection in general IoT networks.
  - **Support Vector Machines (SVM):** Used to identify optimal hyperplanes for classifying malicious device masquerading.
- **Non-Linear Models:**
  - **Random Forest (RF):** An ensemble approach that reduces bias and variance, frequently used to detect sinkhole attacks in IoT routing.
  - **Extreme Gradient Boosting (XGB/EGB):** Highly efficient for parallel tree-boosting, used for detecting Botnet attacks with high accuracy.

    K-Nearest Neighbors (KNN): Useful for handling uncertain data stored in semi-trusted cloud servers.

Performance Metrics

The performance of these intelligent systems is measured through several key indices:

1. **Accuracy:** The ratio of correct predictions to the total predictions.
2. **F1-Score:** The harmonic mean of precision and recall, critical for binary classification in security.
3. **Cohen Kappa Score:** Measures accuracy relative to random chance, with 1 being ideal.
4. **Matthews Correlation Coefficient (MCC):** Contrasts observed and predicted binary classifications on a scale of -1 to 1.

Case Study: Earthquake Early Warning System (EWS)

To demonstrate the practical application of NSAI and Intelligent Systems, we consider an IoT-based Earthquake EWS**.**

System Integration: This system merges cellular networks, social networks, and IoT sensors to mitigate seismic disasters. **The Role of AI:**

- **Pre-disaster Phase:** ML models are used for **"picking,"** which is exactly locating the start of the primary seismic wave before the destructive wave arrives. This allows for the quick shut-off of energy generators and nuclear power plants.
- **Post-disaster Phase:** Intelligent systems facilitate the compilation of reliable data regarding impacted individuals and geographic areas to execute a successful evacuation strategy.
- **Security Needs:** ML plays a vital role in ensuring data privacy and detecting malicious behavior that could lead to fraudulent alerts or a sabotaged evacuation plan.

Through the IoT system, seismic activity is detected and securely transferred to the data processing stage where ML models run the protection process and deliver decisions back to railway systems and utility grids for execution.

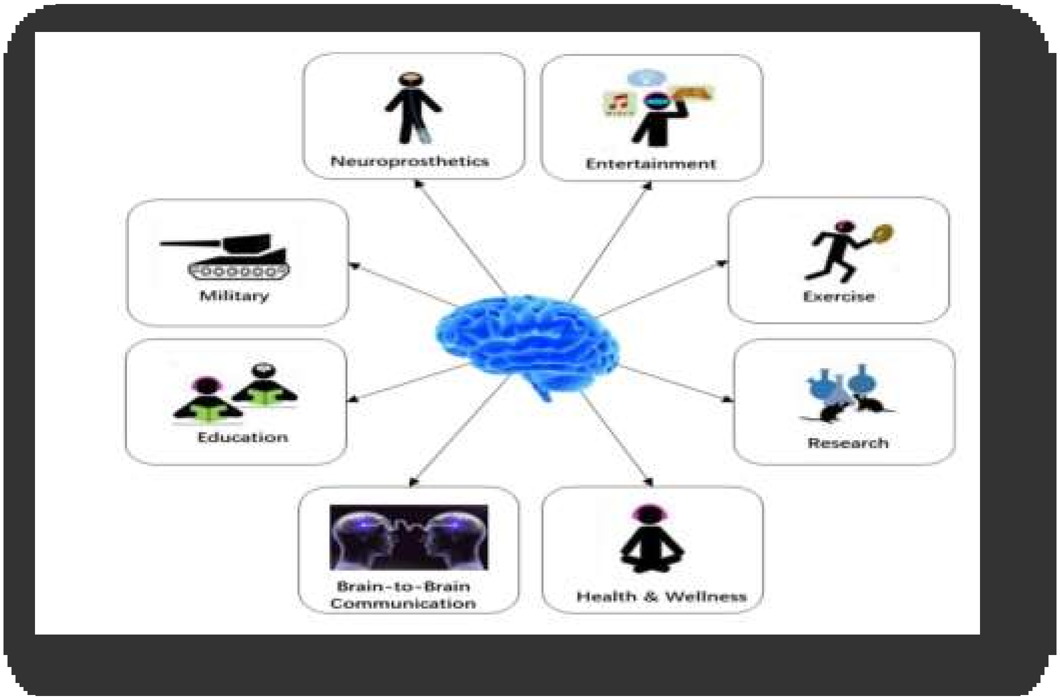
Conclusion:-

The integration of AI into networking represents a transformative step toward a unified IT revolution, merging cyberspace with the physical world. By adopting the NSAI framework, we can overcome the resource limitations of individual devices through distributed intelligence and decentralized trust. This paper has demonstrated that while IoT security faces significant hurdles—such as default credentials and legacy systems—emerging technologies like Federated Learning and Blockchain provide a robust path forward for intelligent systems.

Future Scope:

The ultimate vision for intelligent systems is the transition from NSAI toward Ubiquitous Brain Networks (UBN)**.**

- **Roadmap to UBN:** Future systems will integrate human intelligence agents into the network through **AI-**empowered Brain-Computer Interfaces (ABCI)**,** allowing for "telepathic" communication and the networking of multiple brains to solve complex global problems.
- **Online Evolutive Learning (OEL):** Transitioning away from supervised learning toward OEL will allow AI entities to generate new knowledge by exchanging information among themselves without human data labeling.
- **Quantum Resilience:** Research must focus on developing quantum-resistant cryptography to protect IoT data integrity against future computational threats.
- **Super Power Efficiency:** Bridging the gap between electronics and the human brain's power efficiency remains a critical challenge for the future "AI Society".



References:-

1. "IoT Security: Principles, Practices, and Future Frontiers," Future Internet (2024).
2. "Consumer, Commercial and Industrial IoT (In)Security: Attack Taxonomy and Case Studies."
3. Song et al., "Networking Systems of AI: On the Convergence of Computing and Communications," IEEE.
4. "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories" (2025).
5. "A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions," ACM Computing Surveys (2023).
6. Abdalzaher et al., "Toward Secured IoT-Based Smart Systems Using Machine Learning," IEEE Access (2023).