INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

A Secure Framework for IoT Applications Using Blockchain and Artificial Intelligence

Tina Yadav, Ravindra Chauhan

Deptt. of Computer Science & Engineering, R.D Engineering College Ghaziabad Uttar Pradesh India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1407000046

Abstract - This research addresses key security and privacy challenges in IoT by proposing a multi-layered security framework. It includes formal verification of IoT protocols using the Scyther tool for secure communication, a hybrid intrusion detection system using LSTM and Deep Reinforcement Learning, and an ensemble model combining CNNs with a Quantum Neural Network to improve detection accuracy. Additionally, a blockchain-based system with Improved PCA and a GRU–Deep Belief Network classifier enhances accuracy and reduces false positives. Experiments demonstrate strong performance, with detection accuracy up to 97.26% and improved reliability through blockchain integration.

I. Introduction

Recently, the internet's primary function has been connecting computers anywhere at any time, but this requires human supervision and contact. IoT gives the current communication technologies (ICTs) and information a new dimension by expanding communication capabilities to include "Anything communication." The IoT connects physical and virtual things, enabling anytime, everywhere connectivity for anything [22]. In the IOT, physical and virtual objects communicate simultaneously in space and time [l]. The term "IoT" may have many meanings because the IoT is the culmination of technology advancements in numerous domains, including embedded systems, wireless sensor networks, ubiquitous computing, mobile computing, and machine-to-machine communication. Although there are multiple definitions of the IoT in the literature, the ITU defines it as the system of interconnected physical objects or things that allows data collection and exchange. These "things" include electronics, software, sensors, and network connectivity.

The IOT is defined by McEwen and Cassimally using the straight forward equation: "Physical Actuators + Internet = IoT in 2014.

II. Literature Review

Intrusion Detection Systems (IDS) have evolved in the IoT context, tackling diverse attack types and architectural challenges. The reviewed literature has been categorized into six key domains based on attack type, infrastructure, and detection strategy.

DoS Attack Detection Techniques

Researchers have explored various strategies to detect and mitigate Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks in IoT networks:

SDN-based Models: Bhayo et al. (2020) developed C-DAD, an SD-IoT security framework that dynamically detects DDoS attacks using programmable network metrics. Dao et al. (2021) further improved this with FOGshield, a fog-based collaborative defense architecture leveraging federated learning.

Machine Learning Approaches: Jia et al. (2020) achieved high DDoS detection accuracy (98.9%) using LSTM-based models trained on a composite dataset. Anthi et al. (2021) introduced adversarial machine learning to test IDS robustness under hostile data inputs, observing a significant drop in detection performance.

Rule and Anomaly-Based Techniques: Doshi et al. (2021) proposed anomaly-based IDS suited for emerging DDoS variants targeting mobile and wearable IoT devices.

Context-Aware Protocols: Maati and Saidouni (2020) focused on middleware protocols enabling contextual service restoration in SOA-based hybrid IoT systems.

Fog-Based Models

Fog computing has enabled near-device intelligence for real-time intrusion detection:

Collusion Attack Detection: Yaseen et al. (2017) proposed a fog-based detection framework for mobile IoT environments to detect collusion attacks, leveraging SDN for flexible design.

Fuzzy Logic-Based Models: Zahra and Chishti (2020) developed FLFSioT, combining fog computing with fuzzy logic to enhance detection accuracy and reduce edge-node latency.

Privacy-Preserving Aggregation: Amuthan and Sendhil (2020) introduced HGSW-DM-FHE to resist data injection attacks by ensuring resilient data aggregation at the fog level.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Hybrid Classification Models: Souza et al. (2020) implemented a two-step hybrid DNN-kNN model using NSL-KDD and CICIDS2017 datasets to classify attack types efficiently.

AI-Based IDS Techniques

AI methods are increasingly adopted to address evolving attack patterns in IoT:

Perception-Layer Anomalies: Nasralla et al. (2020) used dynamic time-warping for time-series anomaly detection in smart furniture environments.

Insider Threat Detection: Khan et al. (2019) applied lightweight AI models to detect anomalies from constrained IoT sensors.

Data Imbalance Handling: Karthik and Kumar (2021) employed RF-SMOTE to improve classification on imbalanced datasets like NSL-KDD and N-BaIoT.

Trust-Based Learning Models: Prathapchandran and Janani (2021) proposed RFTrust for detecting RPL-specific sinkhole attacks.

Deep Learning Ensembles: Tsogbaatar et al. (2021) developed DeL-IoT, a comprehensive deep ensemble learning framework incorporating prediction and anomaly detection via SDN.

RPL Network Attack Detection Systems

Routing Protocol for Low-power and Lossy Networks (RPL) is a common target for IoT attacks:

Trust-Based Detection: Mbarek et al. (2021) presented a trust-based system to detect replication attacks using network responsiveness as an indicator.

Simulation-Based Analysis: Sharma and Verma (2020) studied the impact of three RPL attacks—Hello flood, version number, and rank attacks—on network efficiency via simulations.

Multi-Instance RPL: Bang and Rao (2021) employed a hybrid strategy with multi-instance RPL and trust-based parent selection for resilience.

HRCA-Based Detection: Kaliyar et al. (2020) introduced methods to detect Sybil and wormhole attacks by analyzing hierarchical relationships among RPL nodes.

Research Gaps and Challenges

Despite the breadth of research in IDS for IoT, several critical challenges remain:

Resource Constraints: Most IoT devices have limited processing power, memory, and energy, making it difficult to deploy conventional or complex IDS models directly.

Protocol Diversity and Stack Limitations: The heterogeneous and often proprietary protocol stacks used in IoT systems limit the portability and adaptability of IDS across platforms.

High Dimensionality and Overfitting: ML/DL-based IDS often suffer from overfitting due to high-dimensional feature spaces, especially when applied to small or imbalanced datasets.

Insider Attack Detection: Most IDS are focused on external threats, leaving insider threats or stealthy behavior largely unaddressed.

Latency and Real-Time Detection: Real-time IDS in fog or edge environments must strike a balance between speed, accuracy, and power consumption.

Blockchain Scalability: While blockchain enhances security, it introduces overhead, latency, and storage issues that may not be suitable for lightweight IoT devices.

Lack of Standardized Datasets: Benchmarking IDS performance is hindered by the lack of standardized, real-world datasets representing modern IoT attacks.

III. Suggested Methodology

Model-Checking M2M and Centralised IoT Authentication Protocols — Concise Overview

Designing trustworthy authentication for IoT networks demands more than traditional validation; it requires **formal, mathematical verification**. This study employs *model checking* with the **Scyther** tool to prove the security of two widely used protocols:

RADIUS-based central authentication (cloud-centred AAA)

CoAP machine-to-machine (M2M) authentication (resource-constrained client/server)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Verification Workflow

Protocol abstraction – RFC specifications for RADIUS (rfc 3579) and CoAP are distilled into security-protocol description language (SPDL) models that define roles, messages, and fresh nonces.

Claim events – Properties such as *secrecy*, *aliveness*, and *non-injective agreement* are expressed as local **claim** statements in temporal logic.

Model checking – Scyther explores the finite state space, seeking counter-examples. If a claim fails, it returns an attack trace; otherwise the property is proven.

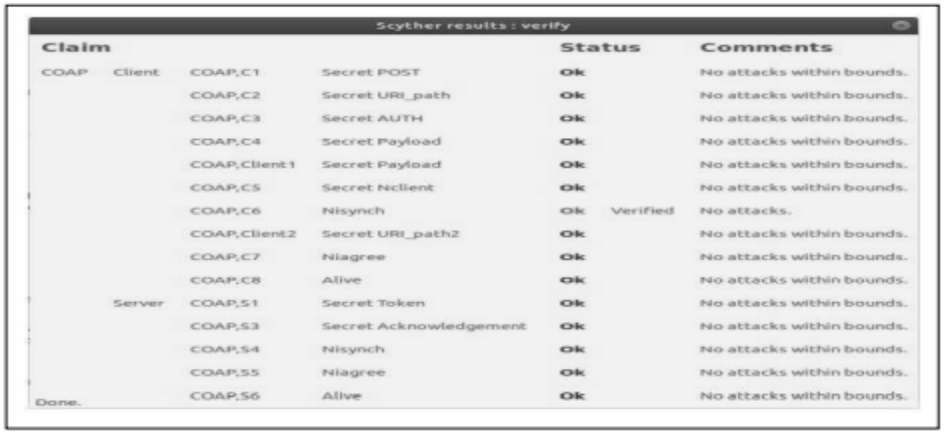

Fig 3.3: CoAp Protocol Verification Result

IV. Results and Discussion

Proposed schemes for Intrusion detection systems in IoT, discussed in previous chapters, are compared with each other. The proposed approaches are investigated for their performance by considering various evaluation metrics, such as Accuracy, Sensitivity, FNR, Specificity, Precision, NPV, Fl-score, and MCC. Table 6.1 shows the results using Database **1,** and Table 7.2 shows the results using Database 2. This work presents four key contributions to enhance IoT security through authentication and intrusion detection:

Formal Protocol Verification: The CoAP and RADIUS IoT authentication protocols were formally verified using the Scyther model checker, ensuring key security properties like secrecy, synchronization, and aliveness.

Hybrid Deep Learning IDS: A combined LSTM and Deep Reinforcement Learning (DRL) model was developed for effective attack detection, using raw features with LSTM and statistical features with DRL.

Deep Ensemble Classification: An ensemble IDS combining CNN1, CNN2, and a Quantum Neural Network (QNN) was proposed to improve detection accuracy and robustness.

Blockchain-Based Detection: A blockchain-supported IDS using DBN and GRU classifiers was introduced, with IPCA applied for optimal feature selection and efficient performance.

A blockchain mechanism-dependent IoT attack detection technique was developed in our fourth contribution, which utilizes hybrid classifiers like DBN and GRU to find IoT attacks. Also, to provide better outcomes by choosing the best features from retrieved features, this approach utilizes IPCA for feature selection.

Table. 1 Comparison of the all the proposed schemes using Db 1

Metrics	HC+SIBRO	ECISF	HC (GRU + DBN)
MCC	0.949195	0.887035	0.879751
Sensitivity	0.973424	0.953356	0.945589
FNR	0.026576	0.016644	0.054411
Specificity	0.970028	0.94368	0.94008
Precision	0.968389	0.943356	0.909367
F1-score	0.9709	0.943356	0.927124
NPV	0.974749	0.92368	0.964506
Accuracy	0.971666	0.964973	0.942221
FPR	0.029972	0.04632	0.05992

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Table 2 Comparison of all the three proposed schemes using Db 2

Metrics	HC+SIBRO	ECISF	HC (GRU + DBN)
Accuracy	0.971666	0.964973	0.942221
NPV	0.974749	0.92368	0.964506
Specificity	0.970028	0.94368	0.94008
F1-score	0.9709	0.943356	0.927124
MCC	0.949195	0.887035	0.879751
Sensitivity	0.973424	0.953356	0.945589
FPR	0.029972	0.04632	0.05992
Precision	0.968389	0.943356	0.909367
FNR	0.026576	0.016644	0.054411

V. Major Findings

The Scyther model checker formally verified RADIUS and CoAP authentication protocols and discovered that both protocols were secure from attacks. For centralized IoT device authentication, the RADIUS protocol works best, and the CoAP protocol can be utilized for secure M2M authentication.

A higher accuracy, which is approximately higher, was atta by the adopted hybrid, classifier + SIBRO for 90LP, while other extant schemes attained lower accuracy than that.

Tattainedposed ECISF attained a low proposal of approximately 0.1,2, which has better findings at 60LP than other systems.

A higher accuracy rating of 97.26 was obtained by utilizing (of GRU + DBN) for the best case at the same time, other approaches attained less accuracy for dbl.

Reference

1. National Research Council. 1999. Funding a Revolution: Government Support for Computing Research. Washington, DC: The National Academies Press. https://doi.org/10.17226/6323.
2. Qi, Lianyong & Khosravi, Mohammad & Xu, Xiaolong & Zhang, Yiwen & Menon, Varun. (2021). Cloud Computing. 10.1007/978-3-030-69992-5.
3. Beri, Rydhm& Singh, Jaspreet. (2020). Cloud computing.
4. P, Krishna Sankar& N P, Shangaranarayanee & Saravanan, K. (2020). Cloud Computing.
5. Manvi, Sunilkumar& Shyam, Gopal. (2021). Cloud Computing: Concepts and Technologies. 10.1201/9781003093671.
6. Kumar, Abhishek &Sanjeevi kumar, P. &kumar, vishal. (2021). Blockchain Security in Cloud Computing. 10.1007/978-3-030-70501-5.
7. P, Krishna Sankar& N P, Shangaranarayanee & Saravanan, K. (2020). Cloud Computing. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france
8. FRAUD THE FACTS 2019 | The Definitive Overview of Payment Industry Fraud
9. John Gantz and David Reinsel, THE DIGITAL UNIVERSE IN 2020: Big Data, Bigger Digital Shadow s, and Biggest Grow th in the Far East, https://www.cs.princeton.edu/courses/archive/spring13/cos598C/idc-the-digital-universe-in-2020.pdf https://www.cloudtp.com/doppler/cloud-economics-getting-bigger-picture/ https://www.vxchnge.com/blog/different-types-of-cloud-computing
10. Hayes, Patrick & Morgenstern, Leora. (2007). On John McCarthy's 80th Birthday, in Honor of His Contributions. AI Magazine. 28. 93-102. 10.1609/aimag. v28i4.2063.
11. David W Cearley, Cloud Computing: Key Initiative Overview, Gartner Report, 2010
12. Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, 7 Oct 2009
13. Dustin Amrhein and Scott Quint, Cloud Computing for the Enterprise: Part 1: Capturing the Cloud, DeveloperWorks, IBM, 8 Apr 2009.
14. Saurabh Chauhan, Dharamveer Singh, Atul Kumar Singh (2022) "Artificial Intelligence in The Military: An Overview of The Capabilities, Applications, And Challenges", Journal of Survey in Fisheries Sciences, Vol 9 (2) pp 984-991. https://doi.org/10.53555/sfs.v9i2.2911
15. Kiran, Dharamveer Singh, Nitin Goyal, (2023) "Analysis Of How Digital Marketing Affect By Voice Search", Journal of Survey in Fisheries Sciences, Vol. 30 (2) 407-412. https://doi.org/10.53555/sfs.v10i3.2890
16. Yukti Tyagi, Dharamveer Singh, Ramander Singh, Sudhir Dawra (2024) "Analysis of The Most Recent Trojans On the Android Operating System", Educational Administration: Theory and Practice, Vol. 30(2) 1320-1327. https://doi.org/10.53555/kuey.v30i2.6846
17. Shivanee Singh, Dharamveer Singh, Ravindra Chauhan (2023) "Manufacturing Industry: A Sustainability Perspective on Cloud and Edge Computing", Journal of Survey in Fisheries Sciences, pp 1592-1598. https://doi.org/10.53555/sfs.v10i2.2889