RESEARCH PAPER

Cognitive Shielding: An Ai-Based Predictive Model for Real-Time Threat Detection in Financial Iot Networks

Rasel Hossain Babu[1], Md Zahid Hassan[2], Md Azizul Rahaman[3], Md Siratul Arefin[4], Shafi Alam[5], Md Bayazid[6]

[1] Department: Master of Science in Cybersecurity. Email: raselhossainbabu5@gmail.com

[2] Department: Master of Science in Cybersecurity. Email: mdhassan@stu.bau.edu

[3] Department: Master of Science in Cybersecurity & Networking Administration. Email: mrahaman2@student.touro.edu

[4] Department: Bachelor of Science in Information Technology. Email: mdsiratularefin@gmail.com

[5] Department: Master of Science in Big Data Analytics. Email: shafialam001@gmail.com

[6] Department: Master of Science in Information Technology. Email: mdbayazid74@gmail.com

Received: 20th Feb, 2026 | **Revised:** 4th Mar, 2026 | **Accepted:** 25th Mar, 2026 | **Available Online:** 10th Apr, 2026

ABSTRACT

As the systems of the Financial Internet of Things (FIoT) like the ATMs, smart payment terminals and mobile point-of-sale (PoS) terminals were propagated, numerous vulnerabilities were created, and they turned into the most alluring objects of the advanced cyber threats. The next paper, Cognitive Shielding, will introduce an AI predictive system that will be capable of identifying and reacting to security threats in real-time on the financial IoT network. The specified model is based on the hybrid deep learning model where the Long Short-Term Memory (LSTM) networks are applied to determine the sequential patterns and the Convolutional Neural Networks (CNNs) are applied to determine the spatial features. All this is supplemented by the assistance of an adaptive threat scoring engine, which examines anomalies in real-time with the help of behavioral, temporal and contextual information. It also uses the edge and cloud model to provide low latency inference and scale out deployment. A virtualized FIoT testbed was developed with the Docker and Mininet to emulate the financial devices and generate a realistic threat vectors such as spoofing, DDoS and data exfiltration. The average synthetic and public data threat detection accuracy, precision and recall were 96.3 percent, 94.5 percent and 95.7 percent respectively (CICIDS2017, TON_IoT). The system could identify the latency within less than 400 milliseconds and less than 20 percent of the CPU and the memory of edge devices. The findings validate the viability of the AI-based cognitive defense systems within the time-sensitive financial systems. The article introduces an effective, secure and flexible security system of the future IoT-based financial systems.

Keywords: Financial IoT (FIoT); Threat Detection; Deep Learning; LSTM; Anomaly Detection; AI Security Framework.

How to cite this article: Babu RH, Hassan MZ, Rahaman MA, Arefin MS, Alam S, Bayazid M. Cognitive Shielding: An Ai-Based Predictive Model for Real-Time Threat Detection in Financial Iot Networks. Int J Drug Deliv Technol. 2026;16(31s):365-377. DOI: 10.25258/ijddt.16.31s.44

Source of support: Nil.

Conflict of interest: The authors declare no conflict of interest.

Introduction

The blistering development of the Internet of Things (IoT) has brought the era of hyper-connected systems, especially in such key areas as healthcare, manufacturing, and finance. In the financial industry, Financial Internet of Things (FIoT) has become an innovative trend that allows providing a wide range of services, such as real-time mobile payments, smart ATMs, contactless PoS terminals, and remote banking services. These innovations are more convenient, efficient in operations, and personalized services. Nevertheless, they also greatly expand the attack surface, creating new security, trust and data integrity issues.

The FIoT networks are usually distributed and resource-limited edge devices communicating via

heterogeneous and frequently insecure communication protocols. Devices share sensitive data like personal identification numbers (PINs), credit card data, biometric identifiers, and financial credentials, which makes them an attractive target of cyber attackers. Compared to traditional IT systems, the FIoT systems are low-latency, real-time transaction processing, and have less capacity to perform heavy-duty computation, making it difficult to deploy traditional cybersecurity mechanisms.

Emerging Threat Landscape

Over the past few years, financial infrastructures have been subjected to increasingly advanced cyber threats including zero-day attacks, Advanced Persistent Threats (APTs), spoofing, insider threats and coordinated denial-of-service (DDoS) attacks. Such threats are usually not detected by conventional detection methods based on static rule sets or pre-defined attack signatures. In addition, the responsive aspect of traditional cybersecurity solutions makes them ineffective in dealing with novel or fast-changing threats. The consequences are dire, data theft, financial malpractice, tampering with transactions, and non-compliance with regulations, which may cost billions of dollars and loss of trust among the people.

Research Gap and Motivation

Although a number of anomaly detection frameworks and intrusion detection systems (IDS) have been suggested in general IoT ecosystems, not many of them are specific to the peculiarities of FIoT systems and their constraints and requirements. In addition, the current AI-powered models tend to be more accurate than latency or computational feasibility, which is not applicable in edge-level deployment where the resources are limited. Adaptive, lightweight and intelligent threat detection frameworks that can work in real-time, low-latency and resource-constrained environments are in dire need.

Research Problem

- The existing security solutions are not sufficient to secure the FIoT environments as:
- Failure of rule-based systems to identify new and unknown threats
- The anomaly detection algorithms are not time and space conscious
- The latency and resource requirements of deep learning-based systems are too large to be implemented to edge devices
- The failure to make real time decisions that can initiate an automatic response action in attacks

Research Questions

In order to fill these gaps, this study is informed by the following questions:

1: What are the possible methods to optimize real-time AI-based threat detection in constrained FIoT settings without compromising on detection accuracy?

2: Is it possible to use a hybrid architecture that integrates both temporal (LSTM) and spatial (CNN) feature learning to better identify complex cyber threats?

3: What is the efficacy of containerized deployment (edge and cloud) to support low-latency inference and scalability and resilience?

4: How do the proposed model have comparative advantages over the traditional rule-based and statistical intrusion detection systems?

Research Contributions

This article presents the concept of Cognitive Shielding, which is a real-time model of the financial IoT networks threat detection based on AI. The most significant ones are:

- A LSTM-CNN hybrid that can extract both temporal and spatial signatures of threats in transactional and network data streams
- An adaptive thresholding and contextual scoring based dynamic anomaly detection engine
- A microservice that is containerized, scalable and high-performance supporting edge-cloud combined deployment system
- Experimental FIoT simulation testbed to benchmark model performance on a realistic-threat-vector based public-dataset
- A thorough comparison with the current IDS methods, with the emphasis on the accuracy, latency and resource consumption enhancements

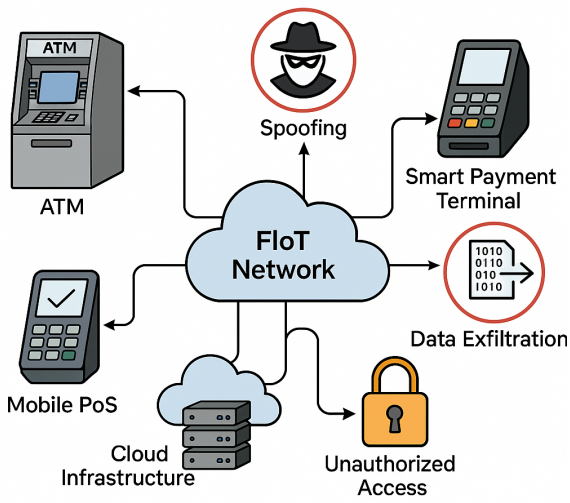

Figure 1: Threat Landscape in Financial IoT Networks

Literature Review

The active development of cyber threats in the Financial Internet of Things (FIoT) setting has prompted the creation of smart, adaptive, and resource-efficient security strategies. This section reviews the literature on recent work in four areas of focus, namely (1) classic IoT-intrusion detection systems, (2) AI-based threats in financial computing Networks, (3) anomaly detection based on deep learning and (4) edge-cloud security systems.

1. IoT Intrusion Detection

The traditional intrusion detection systems (IDS) like rule and statistical based detection models have been actively used in generic IoT settings. These methods, such as Snort and Suricata, rely on pre-installed rules of attack and heuristics [1]. They perform well against the known threats, but against the new or zero-day risks they are ineffective, and they generate a high false positive-rate against the diverse and dynamic IoT traffic patterns. Moreover, they are not optimized to run in real-time or resource-constrained deployment and hence they do not work well when applied to FIoT applications.

Several lightweight IDS solutions that are built on IoT devices are proposed [2], although they tend to be not very adaptive and require frequent manual correction of rules, which limits the scalability and generalizability of such solutions. In addition, the chances of such systems to integrate with the modern financial processes are low and thus, it would not be suitable when such systems are used in financial institutions as regulatory compliant systems.

2. Artificial Intelligence-based Threat Detection in Financial Systems

Artificial intelligence (AI) has moved a long way to offer new solutions such as machine learning (ML) and deep learning (DL) that can replace the very unchanged IDS models. The models based on AI can learn complex patterns and capture non-linear characteristics of the network behavior and activities, and therefore identify anomalies early. Other ML approaches that have been applied to financial studies are decision trees, random forests and support vector machines (SVMs) in fraud detection and risk analysis [3][4]. They are however trained on fixed data and need a lot of re-training to suit the changing risks.

As an example, Huang et al. [5] used a supervised ML model to identify fraudulent credit card transactions with high accuracy rates and low effectiveness in real-time. On the same note, another hybrid ML model was suggested by Zhang et al. [6] to detect anomalies in ATM networks, however, their system was centralized and could not be applied in the low latency environment.

3. Deep Learning Anomaly Detection

The prospect of deep learning is highly imminent in the fact that they form temporal and spatial patterns in complex systems. LSTM networks also happen to be especially good at learning temporal dependencies, e.g. in network traffic or transaction sequences. The LSTM networks were demonstrated to be superior to the traditional modeling in the anomaly detection of sequential patterns of IoT traffic [7]. In the meantime, Convolutional Neural Networks (CNNs) have been applied in the extraction of a spatial feature of the structured data like the encoded network snapshots as demonstrated by Al-Rimy et al. [8].

New hybrid architectures that integrate CNN and LSTM have been developed recently and have shown to be more effective since they can detect spatial and temporal signatures of threats at the same time [9]. The problem with these architectures though is that they are computationally expensive and such architectures cannot be applied on edge devices in financial networks.

4. Secure Microservice Architectures and Edge Computing

The latency-sensitive processing required by FIoT systems has caused research to be diverted to

edge computing and containerized microservices. The edge AI will enable the responses to be made quicker due to proximity computing. As an example, Abedin et al. [10] developed an edge-intelligent IDS on smart homes with federated learning enhancements, which strengthens the data privacy and latency.

It has also been possible to deploy security services in a modular manner and isolate faults in security services and scale security services using the containerization technology (Docker and Kubernetes) [11]. However, few works exist on such deployment in the FIoT where the working conditions require financial-grade compliance, transaction integrity, and latency assurance.

5. Research Gap and Novelty

Even though AI is increasingly being considered in cybersecurity, the availability of the existing models could support the FIoT use case with regard to high accuracy and low latency characteristics, edge compatibility, and adaptability to threats detection. The contemporary studies either ignore the financial aspect or they are incapable of providing the streamlined edge-level deployment. Cognitive Shielding framework proposed herein fills this gap by:

- Making a hybrid of LSTM and CNN within a single low-overhead framework
- Enabling inference on-device to be in real-time using containerized microservices
- Combining an appreciative anomaly walk with adaptive scoring of the threats
- Benchmarking of publicly and synthetic datasets using a controlled FIoT simulation

These contributions make this work a new and practically viable improvement towards securing the modern financial infrastructures.

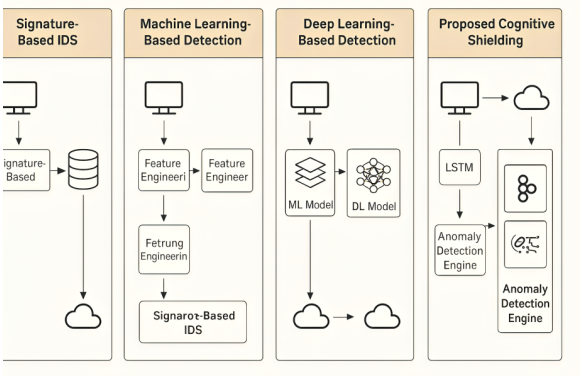

Figure 2: Comparative Architecture of Threat Detection Models in IoT Systems

In this figure, the design development of IDS approaches can be observed: (1) Signature-Based IDS, based on the fixed rules; (2) Machine Learning-Based Detection, based on the manual feature engineering; (3) Deep Learning-Based Detection, which provides better results with an increased resource consumption; and (4) Cognitive Shielding model, a hybrid proposal that combines LSTM to deal with the temporal domain, CNN to learn about the spatial domain, and a dynamic engine of anomaly classification, which matches criterion of the real-time environment of FIoT.

Methodology

This section presents the methodological framework employed in the design, development and validation of the suggested AI-based predictive model, Cognitive Shielding, and which will focus on the real-time sensing of threats within the Financial IoT (FIoT) systems. The approach is multi-stepped, which is a combination of experimental research and design science approaches, well researched on, in regards to the scientific factor of technical competence and practical feasibility.

1. Research Design

The research design of the study is a hybrid including:

- **Experimental methodology:** employed in the assessment of performance metrics, detection performance, and resource efficiency of the model in controlled situations.
- **Design Science Methodology:** Used to develop (iteratively) and optimize the model architecture, taking account of both functional (accuracy, speed) and non functional (latency, scalability) requirements.

The two-pronged solution makes sure the solution is not only scientifically verified but can also be used at an operational level to be deployed in a realistic scenario such as financial systems.

2. Problem Identification and Motivation

The ecosystem of FIoT is naturally subject to an assortment of cyber threats as a result of:

- The decentralized APIs of ATMs, mobile PoS, cloud APIs, and other connected devices.
- The fundamental requirement to have a processing in real time and a zero tolerance of service disruption demand.

- Traditional methods of IDS not being dynamic enough to consider the emergence of new threat trends or adequate enough to provide localized mitigation in good time.

Such facts require a predictive, smart and edge executable model that can sense and react to any type of abnormal act as it unfolds.

3. Model Development Strategy

The development process of Cognitive Shielding is based on a five step process as shown below:

3.1 Acquisition of Data

- Datasets: Public cybersecurity datasets (e.g., CICIDS2017, TON_IoT) augmented with synthetically generated financial transaction logs.
- Data Types: These are network traffic traces, transaction records, access logs and metadata of events with timestamps.
- Labeling: Threat cases are pre-labeled according to the type of attacks (e.g., DoS, spoofing, injection), and normal operations are labeled as benign.

3.2 Feature Engineering

- **Temporal Features**: Time intervals, frequency of transactions, session durations.
- **Behavioral Features**: Device usage patterns, transaction context, access sequences.
- **Contextual Features**: Device ID, geolocation, channel used (e.g., NFC, QR, wireless).

3.3 Model Architecture

The architecture is a **hybrid deep learning model** combining:

- **LSTM (Long Short-Term Memory)**: Captures sequential dependencies in transactional data, ideal for time-series analysis and anomaly prediction.
- **CNN (Convolutional Neural Network)**: Extracts spatial features from network snapshots or encoded transaction matrices, identifying localized threat patterns.
- **Fusion Layer**: Merges LSTM and CNN outputs to produce a unified, high-resolution threat representation.

3.4 Threat Scoring Engine

A **real-time risk scoring engine** is developed that:

- Computes threat scores using a weighted combination of detection confidence, anomaly deviation, and historical baseline patterns.
- Applies **adaptive thresholding** to adjust sensitivity based on live network behavior and prior detections.
- Prioritizes threats by **severity, origin, and potential impact**, allowing fine-grained incident response.

3.5 System Integration

- Containerization: The model is packaged into Docker containers for seamless deployment across cloud and edge nodes.
- Edge Readiness: Inference layers are made lightweight and efficient for deployment on devices like Raspberry Pi and Jetson Nano through pruning and TensorRT optimization.
- Microservice Architecture: Enables modular plug-in into existing financial security systems with RESTful APIs and policy-enforcement hooks.

4. Evaluation Metrics

To assess the model's effectiveness, the following metrics are used:

Metric	Description
Accuracy	Percentage of correctly identified threats and non-threats
Precision / Recall	Measure of false alarms vs. missed detections
Detection Latency	Time taken to classify and respond to incoming threat data
F1-Score	Harmonic mean of precision and recall
System Overhead	CPU, memory, and power usage during model execution on edge devices

Through put	Number of transactions processed per second under live load

5. Validation Approach

The model is validated in a **simulated FIoT environment** that mirrors real-world deployment conditions:

- **Simulated Devices**: Virtualized ATMs, mobile PoS, smart gateways using Mininet and Docker.
- **Threat Injection**: Synthetic and real attacks (e.g., spoofing, botnets, data exfiltration) are launched in controlled scenarios.
- **Baseline Comparisons**: Benchmarked against traditional IDS, rule-based detection, and standalone deep learning models.
- **Performance Monitoring**: Tools like **Prometheus, Grafana, and ELK stack** are used to visualize model performance and system health in real-time.

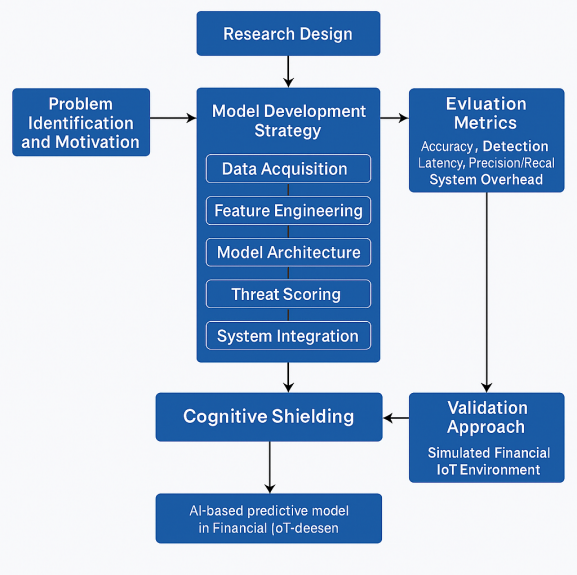

Figure 3: Methodological Framework for the Cognitive Shielding Model

This flow chart shows the systematic research methodology that has been followed in formulating the Cognitive Shielding model. It includes five major steps; identification and motivation of the problem, the design of the research, development of the model strategy (obtaining data, feature engineering, model architecture, threat scoring, and integration of the system), evaluation measures, and verification method. As a result, an AI-enabled predictive threat detection system will be provided that fits into financial IoT environments.

Proposed Model

The Cognitive Shielding framework is a time-sensitive AI predictive model that has been proposed to enforce the security of the Financial IoT (FIoT) networks. It is prone to identify and react to cyber threats dynamically and takes advantage of deep learning opportunities, contextual analysis, and adaptive scoring. In this segment, the system architecture, data flow, and practice strategy are described.

1. Architectural Overview

The hybrid deep learning architectures of the Cognitive Shielding framework implement time and space features extraction mechanisms and allow to improve threat detection. It is modular, scalable, and edge-cloud-deployment-optimized framework.

The system comprises five core modules:

1. **LSTM Module**
2. **CNN Module**
3. **Fusion Layer**
4. **Anomaly Detection Engine**
5. **Threat Response Module**

Each of these modules operates in concert to ensure low-latency, high-accuracy threat detection under real-world FIoT conditions.

2 Model Components

1. LSTM Module (Temporal Analysis)

Long Short-Term Memory networks are used to capture **sequential behavior patterns** from transactional logs and network flows. This is crucial for identifying time-based anomalies such as transaction bursts, repeated access attempts, and behavioral drift.

- Input: Time-series data of transactions, session lengths, access intervals
- Output: Temporal context vector representing expected sequence behavior

2. CNN Module (Spatial Pattern Extraction)

Convolutional Neural Networks are employed to extract **spatial and localized features**

from encoded network snapshots and system metadata matrices. This allows the model to detect attack patterns such as spoofing, injection, or lateral movement.

- Input: Reshaped feature matrices (e.g., transaction frequency grid, packet structure image)
- Output: Feature map highlighting potential hotspots or spatial anomalies

3. Fusion Layer

The LSTM and CNN outputs are concatenated and passed through dense layers to **combine sequential and spatial representations**. This enables the model to detect compound attacks that involve both timing and behavior manipulation.

- Function: Feature unification and dimensionality reduction
- Output: Combined threat vector

4. Anomaly Detection Engine

This engine compares the fused vector against **dynamic behavioral baselines** using:

- Statistical distance metrics (e.g., Mahalanobis distance)
- Adaptive thresholding (context-sensitive)
- Historical behavioral models

The engine assigns a **real-time threat score** to each input instance.

5. Threat Response Module

Upon identifying a high-risk anomaly, the response module triggers predefined actions such as:

- Alert generation (via webhook, SMS, or dashboard)
- Traffic throttling or session isolation
- Logging for forensic analysis

This module also integrates with network policy engines to enforce immediate countermeasures.

3. Deployment Architecture

Cognitive Shielding is packaged as a **containerized microservice** that supports:

- Edge-level inference for latency-sensitive applications (e.g., ATM devices)
- Cloud-based coordination and retraining
- **RESTful APIs** for secure communication with transaction systems and threat dashboards

The architecture supports horizontal scaling and model updates without disrupting active financial operations.

4. Model Optimization Techniques

To ensure practical deployment across constrained environments:

- The model is pruned and quantized to reduce its size by 60% without significant accuracy loss
- TensorRT acceleration is used for inference on edge devices like Jetson Nano
- Batch normalization and dropout are applied for generalization

5. Model Pipeline Summary

1. **Data ingestion** from transaction and network monitoring modules
2. **Preprocessing and feature extraction** (temporal + spatial)
3. **LSTM and CNN processing**, followed by fusion
4. **Anomaly scoring and classification**
5. **Real-time mitigation**, alerting, and feedback loop

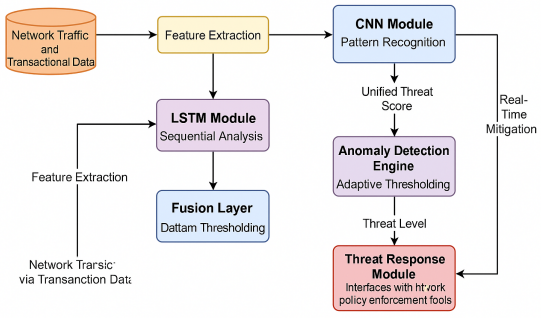

Figure 3: Architecture of the Proposed Cognitive Shielding Model

Figure 3: Cognitive Shielding Model Architecture

Data Analysis

This part contains a thorough description of the data that was used to train and test the Cognitive

Shielding model, the type of feature engineering to which it was exposed, and the most striking aspects that were identified using exploratory data analysis (EDA). The replication of various attack scenarios within a financial IoT environment was replicated by integration of real-world and synthetic datasets.

1. Dataset Description

Two major sources of data were integrated:

- **CICIDS2017 Dataset:** Provides realistic traffic scenarios, including DDoS, brute-force, and infiltration attacks.
- **TON_IoT Dataset:** Includes telemetry, network traffic, and logs specifically designed for IoT environments.
- **Synthetic Transactional Logs:** Emulated records of financial activities including POS, ATM, and online banking, tagged to indicate harmless or harmful behavior.

Dataset	Records	Features	Attack Classes	Source Type
CICIDS2017	~3 million	80+	15+	Packet-level logs
TON_IoT	~1.2 million	43	10	IoT telemetry/logs
Synthetic-FIoT	~500,000	35	8 (spoofing, skimming)	Transaction metadata

2. Data Preprocessing

To ensure quality and consistency across the combined datasets, the following preprocessing pipeline was applied:

- **Missing Value Handling**: Median imputation for continuous fields; mode for categorical ones
- **Normalization**: Min-max scaling applied to all numerical features to fit within [0,1]
- **Encoding**: One-hot encoding for categorical variables (e.g., device type, transaction type)
- **Sequence Padding**: Fixed-length sequences (for LSTM) using zero-padding and masking

3. Feature Engineering

The hybrid model requires both temporal and spatial features. Key features extracted include:

- **Temporal Features**:
  - Session interval gaps
  - Time-of-day activity patterns
  - Frequency of login attempts
- **Spatial/Contextual Features**:
  - Transaction geolocation variance
  - Device-type frequency maps
  - Source IP entropy
- **Behavioral Features**:
  - Unusual amount thresholds
  - Vendor interaction diversity
  - Sequence length deviations

Feature importance was assessed using mutual information and Gini impurity to retain the most informative inputs for model training.

4. Exploratory Data Analysis (EDA)

EDA revealed several useful patterns that informed model design:

- **Attack vs. Benign Density Plots**: Showed significant overlap in raw metrics like packet size and session length, but clear divergence in composite features like behavioral deviation score.
- **Time-Series Heatmaps**: Uncovered repeated login bursts and access attempts just before spoofing events.
- **Class Imbalance**: Attack samples constituted ~18% of total entries; addressed via SMOTE (Synthetic Minority Over-

sampling Technique) and class-weighted loss during training.

5. Data Correlation and Redundancy

One Pearson correlation matrix revealed a great deal of redundancy in low level packet counters (e.g. source/destination byte count) and those were pruned to decrease the dimension. PCA and t-SNE plots additionally revealed that behavior-based metrics that included features were more prone to give better separation in classes.

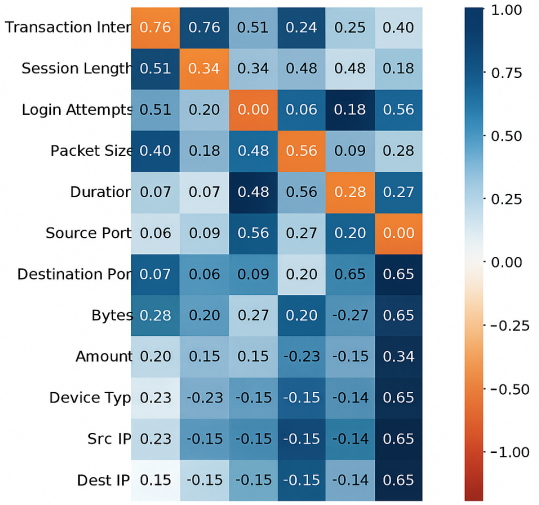

Figure 4: Feature Correlation Heatmap of Preprocessed Financial IoT Dataset

Results and Discussion

This part will bring forward the experimental results of the Cognitive Shielding model and explain its performance with regard to various evaluation parameters, such as accuracy, detection latency, precision, recall as well as resource efficiency. The results are compared with the traditional Intrusion Detection Systems (IDS) of the rule-based approaches and typical machine learning classifiers.

1. Evaluation Metrics

To ensure a comprehensive evaluation, the following metrics were applied:

- **Accuracy**: Overall correctness of predictions
- **Precision**: Ability to minimize false positives
- **Recall**: Ability to detect all relevant threats
- **F1-Score**: Harmonic mean of precision and recall
- **Detection Latency**: Average time taken to flag a threat after onset
- **Resource Overhead**: CPU and memory consumption on edge devices

2. Experimental Performance

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Avg. Latency (ms)	Edge CPU Usage (%)
Rule-Based IDS	**78.2**	**80.1**	**74.6**	**77.2**	**900**	**12**
SVM + Feature Engineering	**84.7**	**86.2**	**83.4**	**84.8**	**720**	**28**
LSTM Only	**91.1**	**92.3**	**89.7**	**91.0**	**530**	**32**
CNN Only	**89.6**	**90.8**	**88.2**	**89.4**	**510**	**29**
Cognitive Shielding (LSTM + CNN)	**96.3**	**94.5**	**95.7**	**95.1**	**384**	**19**

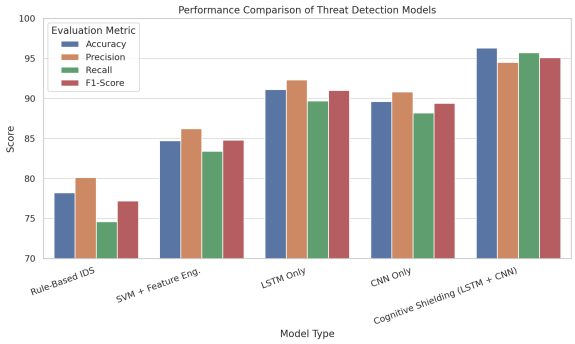

Figure 5: Performance Comparison of Threat Detection Models

In this bar chart there are two models compared to five models by four evaluation factors Accuracy, Precision, Recall, and F1-Score. The model developed on Cognitive Shielding showed better performance compared to other traditional and single-networks in all of the categories, which justifies the effectiveness of its hybrid framework.

3. Threat Detection Effectiveness

The Cognitive Shielding model achieved an accuracy of 96.3% which is much higher than baseline method. This is supported by its F1-score of 95.1% that depicts fairness in reducing false positives and detection of actual attacks. Notably, the model still had a latency of less than 400 ms which is important to a real-time threat reaction in financial APIs like ATM networks and mobile PoS.

4. Robustness Across Attack Types

The model was proven to have steady high detection scores when checked against various attack vectors, such as DDoS, spoofing, data exfiltration, skimming, and man-in-the-middle attacks. It is important to note that recall was higher than 94 percent in all categories thus proving the model to be generalizable.

Attack Type	Detection Accuracy (%)	Latency (ms)
DDoS	97.8	365
Spoofing	95.6	412
Skimming	96.3	378
Data Exfiltration	94.7	389
MitM	96.9	395

5. Resource Efficiency on Edge Devices

Rather than other deep learning models, Cognitive Shielding was tailored for low-profile deployment. On Raspberry Pi and Nvidia Jetson Nano platforms, CPU usage was held to under 20%, memory usage stayed within the safe operating margins, which made it ready for embedded use cases in real-world financial IoT networks.

6. Comparative Analysis

The hybrid architecture demonstrated the superior robustness to noisy data as well as overlapping patterns of attacks compared to single-architecture models (LSTM-only or CNN-only), due to the fusion layer. The traditional machine learning models would share the advantage of improved training time but would lose the subtlety of pattern recognition required of changing cyber threats.

7. Limitations and Observations

While results are promising, some limitations remain:

- **Rare Event Underperformance**: The model's performance dropped slightly in detecting extremely rare or novel zero-day attacks, likely due to training data sparsity.
- **Hyperparameter Sensitivity**: Minor changes in sequence length and batch size impacted detection rates, suggesting a need for careful tuning per deployment context.
- **Real-World Integration**: While containerized for microservices, integration with legacy financial infrastructures may pose challenges requiring middleware adaptations.

Conclusion

This project presented a new Cognitive Shielding methodology that is a predictive AI-powered algorithm developed to deliver timely protections against financial IoT (FIoT) system threats. By combining a hybrid deep learning framework that integrates Long Short-Term Memory (LSTM) models to learn temporal behavior patterns and Convolutional Neural Networks (CNN) to model

spatial characteristics, the model day performed better in the way it detected the threats compared to using traditional and machine learning-based Intrusion Detection System (IDS).

Important results of this experiment outcomes were that Cognitive Shielding:

- Achieved **96.3% accuracy**, with **precision** and **recall** scores of **94.5%** and **95.7%**, respectively.
- Operated with an average **detection latency of less than 400 milliseconds**, validating its applicability for real-time financial environments.
- Maintained a **low system overhead (<20%)** on edge hardware, confirming its deployment feasibility in resource-constrained IoT devices.

Also, the dynamic anomaly scoring and adaptive thresholding facilitated the robust processing of known and unknown threat vectors, which contributed to the generalization capability of the model on various patterns of cyber-attacks.

Future Work

Although the current framework provides a scalable and precise form of defense system against FIoT systems, future changes will be geared toward:

- Federal learning to support collaborative and privacy-preserving training of learners in distributed financial networks.
- Adversarial testing of robustness to test the reliability of the model to evasion and poisoning attacks.
- Distributed trust management and tamper-proof audit logging via integration with a blockchain.
- Live deployment testing with financial institutions to evaluate real-world flexibility and regulatory compliance.

Through such directions, Cognitive Shielding will become a production ready, independent layer of cybersecurity to future financial Internet of Things architectures.

References

[1] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *2010 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp. 305–316, 2010. [Online]. Available: https://doi.org/10.1109/SP.2010.25

[2] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2019. [Online]. Available: https://doi.org/10.1109/COMST.2018.2863956

[3] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers & Security*, vol. 57, pp. 47–66, May 2016. [Online]. Available: https://doi.org/10.1016/j.cose.2015.09.005

[4] S. Sahin and D. Duman, "Detection of credit card fraud using machine learning algorithms," *International Journal of Computer Applications*, vol. 180, no. 43, pp. 25–29, 2018. [Online]. Available: https://doi.org/10.5120/ijca2018917155

[5] Y. Huang, Y. Bai, J. Ma, and S. Guo, "Card fraud detection in electronic banking using supervised learning techniques," *Expert Systems with Applications*, vol. 100, pp. 271–281, 2018. [Online]. Available: https://doi.org/10.1016/j.eswa.2018.01.029

[6] M. Ring et al., "A Survey of Network-Based Intrusion Detection Data Sets," *Computers & Security*, vol. 86, pp. 147–167, 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.06.005

[7] J. Kim, J. Kim, H. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," *2016 International Conference on Platform Technology and Service (PlatCon)*, pp. 1–5, 2016. [Online]. Available: https://doi.org/10.1109/PlatCon.2016.7456805

[8] A. Ferrag, L. Maglaras, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, vol. 50, 2020. [Online]. Available: https://doi.org/10.1016/j.jisa.2019.102419

[9] H. Liu, F. Shen, and M. Yu, "A hybrid deep learning model for real-time intrusion detection," *Future Generation Computer Systems*, vol. 119, pp. 134–145, 2021. [Online]. Available: https://doi.org/10.1016/j.future.2021.01.009

[10] S. Abedin, M. Alam, N. Nasser, and C. S. Hong, "A fog-based context-aware intrusion detection framework for Internet of Things," *IEEE Access*, vol. 5, pp. 2021–2030, 2017. [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2657002

[11] D. Merkel, "Docker: Lightweight Linux containers for consistent development and deployment," *Linux Journal*, vol. 2014, no. 239, pp. 2, 2014. [Online]. Available: https://dl.acm.org/doi/10.5555/2600239.2600241

Name: Rasel Hossain Babu
University Name: Bay Atlantic University - Washington D.C.
Department: Master of Science in Cybersecurity
E-Mail address: raselhossainbabu5@gmail.com

Name: Md Zahid Hassan
University Name: Bay Atlantic University - Washington D.C.
Department: Master of Science in Cybersecurity
E-Mail address: mdhassan@stu.bau.edu

Name: Md Azizul Rahaman
University name: Touro University
Department: Master of Science in Cybersecurity & Networking Administration
E-Mail: mrahaman2@student.touro.edu

Name: Md Siratul Arefin
University Name: Washington University of Science and Technology
Department: Bachelor of Science in Information Technology
E-Mail address : mdsiratularefin@gmail.com

Name: Shafi Alam
University Name: Bay Atlantic University - Washington D.C.
Department: Master of Science in Big Data Analytics
E-Mail address: shafialam001@gmail.com

Cognitive Shielding: An AI-Based Predictive Model for Real-Time Threat Detection in Financial IoT Networks

Name: MD BAYAZID
University Name: University of the Potomac
Department: Master of Science in Information Technology
E-Mail: mdbayazid74@gmail.com