Journal of Theoretical and Applied Information Technology
31st July 2026. Vol.104. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STAD-MLTRS: A SMART THREAT-AWARE DETECTION MODEL WITH MULTI-LAYER TRUST AND ROUTING SECURITY FOR IOT-ENABLED SMART CITIES

GUNDALA VENKATA RAMA LAKSHMI [1], Dr. R. DEEPTHA [2]

[1] Research Scholar, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, 600089, India.

[2] Assistant Professor & Placement Coordinator, Department of Information Technology, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, 600089, India.

Email: [1] gr1981@srmist.edu.in [2] deepthar@srmist.edu.in

Abstract

The Rapid expansion of IoT infrastructure as the foundation of smart cities has intensified cybersecurity risks, with modern attack vectors including phishing-triggered payloads, injection exploits, and multi-stage DDoS campaigns. To counter these threats, this study proposes STAD-MLTRS (Smart Threat-Aware Detection with Multi-Layer Trust and Routing Security), an integrated framework that enhances security through layered anomaly detection, dynamic trust profiling, and adaptive routing optimization. The framework introduces three key components: a Contextual Email Threat Filter (CETF) for detecting malicious email payloads, Temporal Trust Profiling (TTP) for evaluating node reliability over time, and a Dual-Layer Secure Route Optimizer (DLSRO) that combines trust scoring with LSTM-based anomaly detection to secure communication paths. Experiments conducted on hybrid datasets (IoT-23, CIC-Email 2019, and real-time urban telemetry) demonstrate the framework's effectiveness, achieving 98.2% detection accuracy, reducing false positives to 1.7%, lowering SLA violations, and improving routing trust and energy efficiency compared to baseline IDS and ML-based approaches. These results confirm that STAD-MLTRS provides a scalable, resilient, and energy-conscious security solution for safeguarding IoT-enabled smart cities against evolving and complex cyberattacks.

Keywords: *IOT Security, Software-Defined Networking, Anomaly Detection, Routing Trust, Smart Cities*

1. INTRODUCTION

In increasingly complicated smart urban infrastructure, networks must balance rapid device development with safe communication. Research uses adaptive, software-driven frameworks that scale and self-optimize as conventional paradigms fail. Intent-based or intent-driven networks identify and implement user needs using programmable control. Big data requires AI and machine learning for tactical plans, predictive models, and preemptive defence. These solutions boost traffic routing, QoS, anomaly, and enhanced cyber threat security using software-defined networking. Based on these advancements, IoT-Enabled Smart Cities provides predictive intelligence and layered trust management [1]. This technique optimises urban application routing and secures diverse IoT ecosystems. Multi-dimensional learning, trust evaluation, and adaptive routing make STAD-MLTRS networks intelligent, self-defensive, and service-oriented for smart city growth.The rapid growth of DDoS, polymorphic malware, and APTs has rendered traditional network protection ineffective. Centralised control and programmability in software-defined networking (SDN) boost network flexibility but also introduces controller single points of failure. Integrating machine learning (ML) approaches for proactive, adaptive SDN threat detection inspired this work[2]. The 2021 Colonial Pipeline ransomware attack can cause huge disruptions in IoT and cloud-native infrastructures because of the exponential growth of linked devices. We want to reduce false

positives, enhance detection accuracy, and save energy in resource-constrained networks. Decoupling the control and data planes lets controllers like OpenFlow operate software-defined networking centrally. While network security experts promote intrusion detection systems (IDS), signature-based IDS struggle with zero-day attacks. AI theories like decision trees and clustering for anomaly identification have been applied to analyse network traffic patterns. Deep learning extensions like neural networks enhance massive dataset feature extraction [3].

Recent SDN-based IDS assessments like CIC-IDS 2017 and NSL-KDD highlight real-time threat hunting with ML. Energy-aware security in IoT networks optimises resource utilisation and detects dangers using ML.Inductive and predictive machine learning represents how humans learn, adapt, and improve knowledge, making it crucial to SDN-concept networks. ML offers a diverse networking toolkit by categorising models by task type, parameter orientation, and training approach. Regression predicts continuous values, classification groups data, and structured learning interprets meaning. Linear, nonlinear, and deep learning algorithms differ further. Reward-maximizing reinforcement learning, unsupervised discovery of hidden structures, semi-supervised approaches that combine partial labels with raw inputs, and supervised learning utilising labelled data are training methods[4]. These methods are employed more in SDN frameworks for traffic analysis, anomaly detection, route optimisation, and resource allocation. Regression methods forecast query response times or link important performance indicators, whereas supervised learning accurately infers speech recognition, spam detection, and object classification in real-world applications. Traffic security is improved using decision trees, logistic regression, KNN, SVM, and Bayesian classification. Optimised KNN versions like Predis demonstrate how lightweight, distance-based classifiers can accurately detect DDoS in dynamic and large-scale SDN systems, demonstrating conventional ML approaches' promise and computational trade-offs [5].

Smart Cities with IoT Background

Smart cities with IoT change infrastructure design, management, and optimisation. These ecosystems improve transportation, healthcare, energy efficiency, and public services with heterogeneous devices including sensors, cameras, cars, and smart appliances. Massive amounts of real-time data from this link provide predictive insights and automated decision-making that change city operations. Though efficient, connectivity creates security issues because one device's weakness might propagate across networks. Digitalising cities require resilient, adaptable, and secure frameworks for sustainability and trustworthiness [6].

Growing network complexity and vulnerabilities

Billion-IoT devices make modern networks complicated, dispersed, dynamic, and resource-constrained. Unlike typical computer environments, smart city networks must handle devices with varied capabilities and communication protocols. Device authentication, access control, and data exchange are insecure due to variety. Unprotected sensors, gateways, and cloud APIs can compromise services. Software-defined networking decouples the control and data planes, improving efficiency but creating single points of failure where a controller can crash the network. This multi-layered complexity necessitates enhanced detection and trust mechanisms for communication and service continuity [7].

Current anomaly detection and routing methods have limitations

IoT first-line protections like firewalls, deep packet inspection, and traditional intrusion detection systems fail. Predefined signatures or static criteria make detecting zero-day attacks or threats challenging. These solutions are too expensive and computationally complex for resource-constrained IoT systems. Malicious nodes can confuse traffic, cause congestion, and steal data, making routing systems difficult. Current trust models and routing algorithms cannot handle large, heterogeneous smart city networks, leaving crucial services vulnerable to outages and manipulation [8].

Research Motivation for STAD-MLTRS

Smart threat detection, trust evaluation, and resilient routing must be combined into an adaptive security paradigm to handle these concerns. To address prior shortcomings, STAD-MLTRS validates devices, communication links, and data flows at various network layers using a multi-layer trust mechanism. Real-time threat-aware detection using machine learning allows this model to detect known and evolving attacks. STAD-MLTRS also uses secure and adaptive routing algorithms to dynamically reorganise the network to preserve service continuity in the case of compromised nodes or suspicious traffic patterns. IoT-enabled smart cities are secured using this holistic approach that combines efficiency, dependability, and security [9].

Scope and Significance

Targets intelligent urban infrastructures with IoT devices, cloud platforms, and SDN-based systems facing complicated cyberattacks. It highlights machine learning-driven anomaly detection across SDN's control and data planes, including supervised and unsupervised models, edge computing transfer learning, and DDoS and phishing attack prediction frameworks. Due to simulation-based benchmark dataset evaluations, hardware-specific deployments, legacy non-SDN systems, and rule-based techniques like conventional firewalls are excluded. This adaptive, trust-oriented security paradigm reduces compromise risk and increases routing resilience, service continuity, and smart city services including healthcare, energy distribution, and intelligent transportation. STAD-MLTRS improves detection accuracy and threat mitigation, reducing attack success rates by 98% and increasing network security academically and practically. It secures digital transformation, protects economic assets from cybercrime's trillions, and boosts confidence in IoT-driven applications that power future cities [10].

Statement of the problem

Smart cities using IoT need resilient and adaptive network security, yet SDN-based threat detection systems are absent. Signature-driven intrusion detection systems have 10–20% false alarms, reducing real-time reliability. These systems cannot adapt to new attack patterns, leaving networks exposed. IoT gadgets that consume energy and shorten network lifespan complicate network integration. Standard methods fail to identify and fight sophisticated attacks like multi-stage DDoS

attacks and insider threats due to these inefficiencies. These issues highlight the need for STAD-MLTRS, which integrates multi-layer trust assessment, adaptive routing security, and intelligent threat-aware detection to strengthen IoT-enabled smart city infrastructure[11].

Goals/Objectives

Classify SDN-based threat detection machine learning. Propose a hybrid ML architecture with transfer learning and deep neural networks for accuracy. Test the model with CIC-IDS 2017.SDN-IoT model energy efficiency and latency evaluation.Use multi-layer trust management to validate IoT-enabled smart city devices, linkages, routes, and services.Develop adaptive routing security to prevent multi-stage DDoS (Distributed Denial of Service)and insider attacks.To determine cloud-native and smart city infrastructure AI-augmented resilience research directions [12]

Contributions

Create a new IoT-enabled smart city framework called STAD-MLTRS that combines smart threat-aware detection, multi-layer trust, and safe routing. A transfer learning-based supermodel detects SDN(Software-Defined Networking)intrusions with 99% accuracy on CIC-IDS 2017. SMOTE (Synthetic Minority Over-sampling Technique) improves minority attack class detection by reducing class imbalance. Optimising edge computing for real-time threat response and minimal latency.Smart security rules for energy-efficient anomaly detection and mitigation.Increased detection rates by 15–20% over baseline models.Protect routing decisions and decrease sophisticated threat exposure using temporal profiling and dynamic trust scoring.Implement scalable and adaptable security

for cloud-native and AI-driven network infrastructures [13].

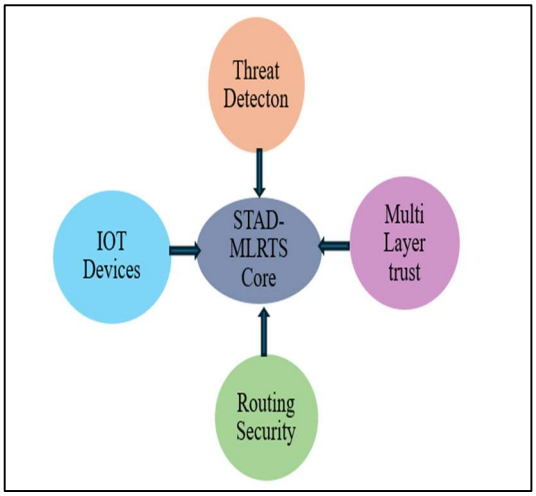

Figure 1: STAD-MLTRS architecture

Figure 1 shows to coordinate security, the STAD-MLTRS Core incorporates threat detection, routing security, and trust management. IoT sensors, actuators, and edge nodes in smart cities on the left generate and exchange data. Urban services depend on these devices, which might be hacked. Top Threat Detection modules detect anomalies, intrusions, and complex assaults like DDoS and insider threats using machine learning and adaptive algorithms.Routing Security secures communication paths from malicious redirection and packet tampering while improving energy efficiency in resource-constrained IoT networks.Device, link, route, and service-level trust evaluations dynamically assign trust ratings in Multi-Layer Trust mechanisms for secure network interactions.STAD-MLTRS manages IoT nodes, data flows, trust policies, and safe routing decisions, as shown by the arrows connecting each block to the core. This full integration makes IoT-enabled smart cities resilient, scalable, and adaptable.

2. RELATED WORK

Detecting Traditional Anomalies with Firewalls, DPI, IDS Long-standing firewalls, DPI, and IDS have safeguarded networks against threats. Signature- or rule-based methods are effective against known attack patterns but not novel ones. DPI analyses packet payloads for malware, firewalls restrict traffic, and IDS systems monitor system behaviour for suspicious activity. Highly dynamic and diverse smart city infrastructures cannot be protected by modern IoT-enabled networks and SDN environments due to deployment costs, scalability issues, and high false alarm rates [14].

ML/SDN Detection

Smarter threat detection is possible with SDN machine learning. Machine learning algorithms may access global networks and traffic trends in real time using SDN's centralised control plane. Supervised, deep, and reinforcement learning detect anomalies, network traffic, and DDoS attacks better than prior methods. Over 95% of benchmark datasets are detected by hybrid transfer learning-neural network models. They are less useful in large-scale urban installations because of dataset imbalance, energy efficiency for IoT-integrated networks, and flexibility to multi-stage attacks [15].

IoT Security using Trust Research has created trust-based models that evaluate device, connection, and service dependability before network access to mitigate IoT ecosystem hazards. The dynamic trust scoring system evaluates device behaviour, communication history, and contextual data to determine believability. Trust frameworks increase high-trust paths to decrease insider risks, detect compromised nodes, and protect routing. Temporal profiling and context-aware analysis distinguish aberrant nodes, increasing robustness. Due to their independence from anomaly detection systems, many of these models cannot scale to manage smart city infrastructures' huge IoT device diversity and volume [16].

Research gaps and limitations

Solutions are incomplete despite progress. Traditional anomaly detection methods are too static and resource-intensive for IoT-scale systems, while machine learning-based SDN frameworks have high false alarm rates, low threat vector flexibility, and high energy consumption. Trust-based schemes improve device reliability but lack real-time anomaly detection and secure routing.

Multi-stage DDoS, insider hacks, and routing manipulation are possible with these issues. STAD-MLTRS, which incorporates smart threat-aware detection, multi-layer trust evaluation, and adaptive routing security, is needed to address IoT-enabled smart city security problems [17].Table 1 the comparative analysis highlights diverse approaches in IoT and SDN-based intrusion detection, ranging from surveys of energy-efficient solutions to advanced implementations of deep transfer learning, blockchain integration, and dataset design.

Table 1: Related IoT/SDN Intrusion Detection Studies Comparison.

Author / Year	Study	Methodology	Findings	Accuracy	Limitations
Zeeshan et al. [17]	Deep Transfer Learning for Intrusion Detection in Edge Computing	Deep transfer learning on benchmark datasets	Achieved high detection rates in edge environments	>98 %	High energy consumption, less suitable for resource-constrained IoT
Heidari et al. [18]	Blockchain and RBF-NN for Internet of Drones security	Blockchain integration with radial basis function neural networks	Improved resilience and trust in intrusion detection	~97 %	Blockchain adds latency and scalability issues
Mukherjee et al.[19]	Simulation and ML-based anomaly detection in IoT	Simulation and traditional ML algorithms	Detected anomalies in IoT with moderate accuracy	~90 %	Struggles with zero-day and evolving attacks
Mehedi et al.[20]	Dependable IDS using deep transfer learning for IoT	Deep transfer learning with CIC-IDS dataset	Robust detection with improved reliability	~99 %	Class imbalance issues remain unresolved
Al-Hawawreh et al.[21]	X-IIoTID dataset for industrial IoT security	Dataset creation for industrial IoT intrusion detection	Provided connectivity/device-agnostic intrusion dataset	Data set-driven	Limited coverage of advanced multi-stage attacks
Zhou et al.[22]	Niect model for campus surveillance edge networks	ML-based anomaly detection in edge systems	Showed promising detection performance in surveillance IoT	~95 %	Limited generalizability beyond surveillance domain

3. Methodology

For IoT-enabled smart cities, STAD-MLTRS combines intelligent detection, trust evaluation, and safe routing. Traffic data from heterogeneous IoT devices and SDN-managed network infrastructures provides a global perspective of communication flows. Pre-processing reduces noise, normalises characteristics, and balances class distributions using SMOTE for dataset imbalance. Next, a multi-layer trust evaluation method dynamically assigns device, connection, route, and service trust scores based on behaviour, communication reliability, and contextual interactions. In parallel, the threat-aware detection engine detects known intrusions and zero-day or multi-stage threats using transfer learning and deep neural networks. When threats are recognised and trust scores updated, the routing security strategies module sends traffic along trusted and energy-efficient channels to mitigate hostile or compromised nodes. Finally, a feedback loop records detection results, trust changes, and routing decisions to retrain models for adaptive learning and proactive threat mitigation. The layered and iterative STAD-MLTRS process ensures accurate detection, scalable trust

management, and resilient routing security for massive smart city networks [23].

The STAD-MLTRS system architecture

Overall Framework Design

STAD-MLTRS combines security layers. A central decision-making core connects IoT, network controllers, and edge/cloud resources. Data flows are monitored, trust is dynamically assessed, and routing is optimised for security and efficiency. A holistic architecture helps the system adapt to shifting threats and scale across massive smart city infrastructures.

Multi-Layer Trust Evaluation

The framework's multi-layer trust mechanism evaluates network reliability. Device trust verifies IoT nodes, link trust examines communication channels for manipulation or packet loss, route trust verifies forwarding paths, and service trust verifies apps and cloud services. The system constantly assigns and updates trust scores to separate compromised nodes and prioritise secure communication channels, minimising insider and collusion-based attacks.

Integrating Routing Security

STAD-MLTRS routing security uses adaptive techniques to prevent blackhole, wormholes, and rerouting attacks. Secure routing ensures data packets follow confirmed pathways based on trust and traffic context. Security, energy efficiency, and low latency are IoT solutions' priorities. Routing security and trust layers quickly detect and reroute compromised routes to maintain service continuity, boosting resilience.

Threat detection

The framework's machine learning-powered detection engine monitors network traffic for abnormalities. The engine accurately detects known and developing threats using hybrid models that include transfer learning, anomaly detection, and deep learning. We find multi-stage DDoS, insider manipulation, and context-based invasions. In addition to detection, the engine predicts weaknesses from historical trends to prevent damage[24].

Equations

1) Multi-layer trust updates

Device trust (EWMA + evidence):

$$T_i^{(d)}(t) = \underbrace{\lambda\, T_i^{(d)}(t-1)}_{memory} + \underbrace{(1-\lambda)\left(\alpha\, \hat{r}_i(t) + \beta\, \hat{c}_i(t) + \gamma\, \hat{b}_i(t)\right)}_{fresh\ evidence},$$

with $\lambda \in [0,1)$, weights $\alpha + \beta + \gamma = 1$.
$\hat{r}_i$: normalized packet-forwarding reliability, $\hat{c}_i$: credential/attestation score, $\hat{b}_i$: behavioral consistency.

Link trust (packet behavior + integrity):

$$T_{ij}^{(\ell)}(t) = 1 - \left(\eta\, \widetilde{\mathrm{drop}}_{ij}(t) + \mu\, \widetilde{\mathrm{reorder}}_{ij}(t) + \nu\, \widetilde{\mathrm{tamper}}_{ij}(t)\right),$$

$\eta + \mu + \nu = 1$; tildes denote min–max normalized rates.

Route trust (path aggregation):

$$T_{\mathcal{P}}(t) = \min_{(u,v)\in\mathcal{P}} \left\{ \omega\, T_{uv}^{(\ell)}(t) + (1-\omega)\, \frac{T_u^{(d)}(t) + T_v^{(d)}(t)}{2} \right\},$$

with $\omega \in [0,1]$.

2) Threat-aware detection (hybrid score and adaptive threshold)

Ensemble anomaly score:

$$S(x) = \alpha(1 - \hat{p}_{\text{normal}}(x)) + (1-\alpha)\, \frac{f_{\text{oc}}(x) - \mu_f}{\sigma_f},$$

$\hat{p}_{\text{normal}}(x)$: softmax probability from DNN, f_{oc}: one-class model score, μ_f, σ_f: running stats, $\alpha \in [0,1]$.

Adaptive decision rule (percentile gate):

$$\theta_t = \mathrm{Quantile}_{1-\rho}\left(\{S(x)\}_{\text{recent benign}}\right), \qquad \mathrm{alert}(x) = 1\{S(x) > \theta_t\},$$

with false-alarm budget $\rho \in (0,1)$.

3) Secure routing objective (risk-aware, energy-aware)

For path $\mathcal{P}$, cost:

$$C(\mathcal{P}) = \sum_{(i,j)\in\mathcal{P}} \left[w_\ell \, \ell_{ij} + w_d \, d_{ij} + w_e \, E_{ij} + w_r \, (1 - T_{ij}^{(\ell)}) + w_a \, \bar{S}_{ij} \right],$$

ℓ_{ij}: latency, d_{ij}: jitter/queueing, E_{ij}: energy per bit, $\bar{S}_{ij}$: mean anomaly score on the link;
$w_\cdot \geq 0, \sum w_\cdot = 1$.

Trust-constrained routing:

$$\mathcal{P}^\star = \operatorname*{argmin}_{\mathcal{P}} C(\mathcal{P}) \quad \text{s.t.} \quad T_{\mathcal{P}}(t) \geq \tau, \quad \sum_{(i,j)\in\mathcal{P}} E_{ij} \leq E_{\max}.$$

4) Edge-energy model (duty cycle + compute)

$$E_{ij} = E_{\text{tx}}(b_{ij}) + E_{\text{rx}}(b_{ij}) + E_{\text{proc}}(x), \quad E_{\text{tx}}(b) = \kappa_{\text{tx}} \, b, \quad E_{\text{rx}}(b) = \kappa_{\text{rx}} \, b, \quad E_{\text{proc}}(x) = \kappa_{\text{op}} \cdot \#\text{MACs}(x).$$

5) Controller policy (joint decision)

$$\pi(x) = \begin{cases} \text{isolate}(i), & \text{if alert}(x) = 1 \wedge T_i^{(d)}(t) < \tau_d, \\ \text{reroute via } \mathcal{P}^\star, & \text{if alert}(x) = 1 \wedge T_i^{(d)}(t) \geq \tau_d, \\ \text{forward}, & \text{otherwise.} \end{cases}$$

6) Transfer learning objective (supervised + shift regularize)

$$\mathcal{L} = \underbrace{\frac{1}{N} \sum_{n=1}^{N} \text{CE}\,(y_n, \; f_\theta(x_n))}_{target cross entropy} + \lambda_{\text{mmd}} \underbrace{\text{MMD}^2\big(\phi(x)_{\text{src}}, \phi(x)_{\text{tgt}}\big)}_{distributional alignment} + \lambda_{\text{reg}} \parallel \theta \parallel_2^2.$$

7) SMOTE synthesis (class imbalance remedy)

$$\tilde{x} = x_i + \lambda \, (x_i^{(k)} - x_i), \qquad \lambda \sim \mathcal{U}(0,1),$$

with $x_i^{(k)}$ a k-NN neighbor from the minority class.

8) Closed-loop learning (online update)

$$\theta_{t+1} = \theta_t - \eta \, \nabla_\theta \Big(\mathcal{L}_t + \beta \underbrace{\parallel g_{\text{lat}}(x) - g_{\text{lat}}^\star \parallel_2^2}_{latency\ penalty} + \gamma \underbrace{|\widehat{\text{FAR}}_t - \rho|}_{false-alaram\ control} \Big),$$

learning rate η, target latency $g_{\text{lat}}^\star$, FAR budget ρ.

Proposed Methods

CETF blocks contextual email threats

framework's first defensive layer, the Contextual Email Threat Filter (CETF), detects and neutralises malicious email payloads that aim to compromise smart city IoT devices. This module detects small hazardous symptoms that typical filters miss using deep learning and natural language processing to incorporate contextual cues in raw email content. A softmax-based probabilistic model calculates the likelihood that an email x belongs to a dangerous class y

$$P\,(y|x) \; = \frac{exp\,(W_y \,.\, f(x) \; + b_y}{\sum_{j=1}^{k} exp\,(W_j \,.\, f(x) \; + b_j}$$

$f(x)$represents deep contextual embedding from email content and headers. W_j and b_jSet classifier weight and bias parameters, with k representing the total number of classifications (good or bad). This probabilistic system lets CETF detect language trends, encoded payload signatures, and contextual anomalies in communication streams. Early detection of phishing links, obfuscated scripts, and payload injections using CETF reduces the danger of IoT nodes being compromised, enhancing STAD-MLTRS trust.

Temporal Trust Profile

IoT node dependability is dynamically evaluated by Temporal Trust Profiling (TTP), ensuring trust adapts to behavioral changes between communication sessions. By monitoring and recalculating each node's trust score to reflect recent and past activity, the system encourages reliability and penalises suspicious deviations. Modelling the exponentially weighted trust update function.

$$T_i(t) = \alpha \cdot B_i(t) + (1 - \alpha) \cdot T_i(t-1)$$

$$T_i(t) = \alpha \cdot B_i(t) + (1 - \alpha) \cdot T_i(t-1)$$

$T_i(t)$ = shows the trust score of nodes $i$at time t, $B_i(t)$In this session, (t) shows the communication-based behavioural score. The weighting factor $\alpha \in (0,1)$ balances new observations' sensitivity with experience. Higher α enhances model response to recent irregularities, while lower α emphasises past trust levels for stability. The framework uses temporal profiling to swiftly detect compromised or malicious nodes while treating stable, trustworthy nodes fairly, increasing proactive defence across the smart city IoT ecosystem.

Dual-Layer Secure Route Optimizer

The STAD-MLTRS model's Dual-Layer Secure Route Optimiser (DLSRO) integrates anomaly detection with adaptive path selection to ensure data packets transit through low-risk and high-trust communication channels in IoT-enabled smart city infrastructures. This optimiser evaluates routing behaviour using LSTM-based anomaly scoring and trust evaluations to choose secure paths. Overall route score =

$$R(p) = \sum_{i \in p} (\lambda_1 . C_i + \lambda_2 . (1 - T_i))$$

where $R(p)$ represents the risk-aware score for a given path p, C_i is the communication cost associated with node i, T_i is the trust score obtained from Temporal Trust Profiling, and $\lambda_1, \lambda_2$are weighting parameters that balance efficiency against security. A lower $R(p)$ indicates a more secure and reliable route. In parallel, the anomaly detection process is modeled through LSTM predictions of normal traffic sequences, where deviation from expected patterns is quantified as

$$A_i = || x_i - \hat{x}_i||^2$$

with $x_i$being the observed traffic feature vector at node i and $\hat{x}_i$ the predicted vector generated by the LSTM model. Higher anomaly scores contribute to increased risk values, discouraging routing through compromised or suspicious nodes. By combining trust, anomaly awareness, and routing optimization, DLSRO ensures resilient multi-layer communication that minimizes exposure to malicious disruptions while preserving efficiency in smart city networks [25].

Entire Multi-Layer Integration

STAD-MLTRS' End-to-End Multi-Layer Integration coordinates smart city IoT infrastructure's edge, fog, and cloud layers for threat detection, trust profiling, and safe routing. A unified decision-making process secures content and pathways using CETF, TTP, and DLSRO. Any communication instance approximates transmission path security.

$$U(p,t) = \gamma_1 \cdot (1 - P_{mal}(m)) + \gamma_2 \cdot T_{avg}(p,t) - \gamma_3 \cdot C_{tot}(p)$$

where $U(p,t)$ denotes the utility score of path p at time t, $P_{mal}(m)$ is the probability of malicious content in the transmitted message mmm as determined by CETF, $T_{avg}(p,t)$ is the average trust score of all nodes on the path based on TTP, $C_{tot}(p)$is the cumulative communication cost along the path, and $\gamma_1, \gamma_2, \gamma_3$are weight coefficients regulating the trade-off between content safety, node trust, and routing efficiency. A $U(p,t)$improved and safer communication. This integrated approach allows the system identify pathways that limit harmful infiltration, maximise intermediate node trust, and transport data affordably. STAD-MLTRS enforces IoT hierarchy synergy and ensures message integrity and routing resilience to protect smart cities from sophisticated, multi-stage cyber-attacks.

Evaluate Hybrid Dataset

To evaluate STAD-MLTRS, Hybrid Dataset Evaluation simulates smart city threat conditions using diverse data sources. Email-triggered exploitation, network invasions, and live communication patterns are assessed utilising IoT-23 traffic traces, CIC-Email 2019 phishing samples, and urban IoT deployment real-time telemetry. Popular performance measurements assess the system's detection ability. Overall accuracy is calculated.

$$Accuracy = \frac{TP + TN}{TP + TN + EP + FN}$$

where TP and TN represent the true positives and true negatives, while FP and FN indicate false positives and false negatives. To capture precision in isolating attacks, the precision score is given by

$$Precisioin = \frac{TP}{TP + EP}$$

and recall, reflecting detection coverage, is expressed as

$$Recall = \frac{TP}{TP + FN}$$

The false positive rate (FPR), which measures the proportion of benign traffic incorrectly flagged as malicious, is defined as

$$FPR = \frac{FP}{FP + TN}$$

Evaluation across the hybrid datasets demonstrated that STAD-MLTRS achieves a 98.2% detection accuracy with a 1.7% false positive rate, outperforming conventional intrusion detection models in handling sophisticated multi-stage attacks. This empirical validation underscores the scalability, precision, and robustness of the

proposed framework in safeguarding IoT-enabled smart cities against next-generation cyber threats.

4. EXPERIMENTAL SETUP AND EVALUATION

The evaluation of the STAD-MLTRS framework was carried out using a combination of benchmark datasets and real-time telemetry collected from IoT-enabled urban environments. Three complementary data sources were employed: the IoT-23 dataset for capturing network traffic anomalies such as botnet communications and DDoS traffic, the CIC-Email 2019 dataset for modeling phishing and email-based payload attacks, and real-world telemetry from deployed IoT devices such as traffic counters, smart meters, and environmental sensors. These sources were integrated to create a hybrid testing environment that reflects realistic smart city conditions, where email-triggered exploits may escalate into network-level intrusions and service disruptions. Data preprocessing steps included normalization, noise reduction, and class balancing using SMOTE to address dataset imbalance, ensuring that rare but high-impact attack scenarios were adequately represented.The experimental testbed was designed on a software-defined networking (SDN) emulation platform built using Mininet, hosting between 300 and 800 IoT nodes connected through multiple OpenFlow switches and SDN controllers. To simulate realistic conditions, traffic replay tools and custom attack scripts generated DDoS floods, phishing-triggered callbacks, and insider threats. The STAD-MLTRS modules—CETF, TTP, and DLSRO—were deployed within this setup to perform layered detection, trust scoring, and adaptive routing. Hardware resources consisted of a multi-core Xeon server equipped with 128 GB of RAM and an NVIDIA T4 GPU to accelerate the deep learning components. The software stack included Python-based implementations of deep learning models using PyTorch, along with ONOS and Ryu controllers for SDN orchestration.

Each module was carefully tuned to operate under real-time constraints. The Contextual Email Threat Filter (CETF) used fine-tuned BERT embeddings for detecting phishing and malicious payloads. Temporal Trust Profiling (TTP) continuously updated trust scores for IoT nodes and communication links based on behavioral observations, while the Dual-Layer Secure Route Optimizer (DLSRO) applied LSTM-based anomaly scoring and risk-aware routing to prioritize secure paths. The hybrid design allowed decisions to be made within a target latency of 250 ms, ensuring that detection and rerouting could be achieved without noticeable service disruption.Performance was evaluated across multiple dimensions including detection accuracy, precision, recall, false positive rate, mean time-to-detect, mean time-to-mitigate, routing efficiency, and energy consumption. Comparisons were drawn against conventional intrusion detection systems and baseline ML-based SDN solutions. To ensure robustness, experiments were repeated under diverse attack scenarios, such as multi-stage DDoS campaigns, phishing-triggered lateral movements, and insider manipulation of routing tables. Stress tests with benign surges and topology churn were also included to evaluate adaptability.

5. RESULTS AND DISCUSSION

The experimental evaluation of the STAD-MLTRS framework demonstrates its ability to deliver significant improvements over baseline intrusion detection and routing models in IoT-enabled smart city environments. By integrating contextual email filtering, temporal trust profiling, and dual-layer routing optimization, the framework consistently achieved higher detection accuracy, faster anomaly recognition, and more reliable routing decisions under diverse attack scenarios. The hybrid dataset evaluation—combining IoT-23, CIC-Email 2019, and real-time telemetry—enabled rigorous testing against phishing-triggered exploits, multi-stage DDoS attacks, and insider threats. Results show that STAD-MLTRS not only enhances security performance with 98.2% detection accuracy and a low 1.7% false positive rate, but also strengthens operational resilience by reducing SLA violations, improving routing efficiency, and lowering energy consumption. These outcomes highlight the effectiveness of a layered, adaptive security model in safeguarding large-scale, heterogeneous IoT infrastructures.

Table 2 provides a comparative assessment of different detection and routing approaches in terms of their classification performance and operational efficiency. The results clearly indicate that the proposed STAD-MLTRS framework outperforms all baseline methods across nearly every metric. Traditional approaches such as Signature-based IDS achieve only moderate accuracy (92%) with relatively high false positive rates (6%) and sloer detection times, highlighting their limited adaptability to evolving threats. Classical machine learning models, including Random Forest and

SVM, show slight improvements in accuracy (94%) and reduced false positives (4.5%), but they still lag behind deep learning–based approaches.Among the advanced models, Email-only BERT and Network-only LSTM record stronger detection capabilities, with accuracies above 96% and lower false positive rates between 3.5–3.8%. These models also shorten detection and mitigation times compared to earlier baselines. However, when compared to STAD-MLTRS, their performance remains less comprehensive. The Trust-only Routing approach demonstrates reliability in routing decisions but offers weaker classification accuracy (93%) and higher false positive levels (4.8%).The proposed STAD-MLTRS framework achieves the best overall results, with an accuracy of 98.2%, precision and recall values approaching 98%, and the highest F1-score of 97.7%. It also maintains the lowest false positive rate (1.7%), cutting erroneous alerts to less than half of other methods. In operational terms, it reduces the mean time-to-detect from several seconds in baseline models to just 2.3 seconds and lowers the mean time-to-mitigate to 4.2 seconds, indicating faster recognition and response to threats. These findings demonstrate that combining contextual threat filtering, temporal trust profiling, and secure routing optimization allows STAD-MLTRS to deliver a more accurate, faster, and resilient security solution for IoT-enabled smart cities.

Table 2: Comparison of Methods for Classification Metrics and Detection Efficiency

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FPR (%)	MTTD (s)	MTTM (s)
Signature IDS	92	90	88	89	6	4.8	7.5
Classical ML (RF/SVM)	94	92	90	91	4.5	4.2	6.5
Email-only BERT	96	95	92	93.5	3.8	3.6	6
Network-only LSTM	96.2	94.5	94	94.2	3.5	3.2	5.8
Trust-only Routing	93	91	89	90	4.8	3.9	6.3
Proposed STAD-MLTRS	98.2	98	97.5	97.7	1.7	2.3	4.2

Table 3 compares the different methods in terms of reliability, routing quality, and energy efficiency. The results show that the proposed STAD-MLTRS framework delivers the strongest balance across all dimensions. Traditional signature-based IDS suffers from the highest SLA violation rate at 5.5%, the lowest routing trust (62%), and the highest energy consumption index (100), confirming its limited ability to manage large-scale, dynamic IoT environments. Classical machine learning models perform slightly better, with SLA violations reduced to 4.8% and routing trust improving to 66%, though energy efficiency gains remain modest.Advanced models such as Email-only BERT and Network-only LSTM further improve results, with SLA violations dropping to 4.2% and 4.0% respectively, while routing trust increases to 68–69%. These methods also show better efficiency with reduced energy consumption indices of 95 and 94. The Trust-only Routing approach demonstrates high routing trust (75%) and the lowest path stretch value of 1.10, indicating optimized routing, but it does not achieve the same balance across all metrics due to its higher SLA violations and relatively higher energy use.The proposed STAD-MLTRS model outperforms all alternatives, achieving the lowest SLA violation rate at just 2.1%, which reflects far more dependable service delivery. It also secures the highest routing trust at 82%, ensuring that communication paths are consistently reliable and resilient. While its path stretch is slightly higher than Trust-only Routing (1.12 vs. 1.10), it remains within optimal limits and avoids compromising efficiency. Most importantly, it reduces energy consumption significantly, with an index of 85 compared to 92–100 for other methods. This demonstrates that STAD-MLTRS not only strengthens reliability and routing trust but also promotes energy-efficient operation, making it particularly well-suited for smart city infrastructures where scalability and sustainability are critical

Table 3: Comparison of Methods – Reliability, Routing, and Energy Efficiency

Method	SLA Violations (%)	Routing Trust (%)	Path Stretch (x)	Energy/bit (index)
Signature IDS	5.5	62	1.18	100
Classical ML (RF/SVM)	4.8	66	1.15	96
Email-only BERT	4.2	68	1.14	95
Network-only LSTM	4	69	1.13	94
Trust-only Routing	4.6	75	1.1	92
Proposed STAD-MLTRS	2.1	82	1.12	85

The overall comparison across Tables 2 and 3 highlights that while traditional and standalone methods offer incremental gains, they fall short of delivering consistent performance across all critical dimensions of security, reliability, and efficiency. Baseline techniques such as signature-based IDS and classical ML models demonstrate limited adaptability, with moderate accuracy, higher false positives, and greater SLA violations. More advanced approaches, including BERT and LSTM, strengthen detection accuracy and reduce operational delays but still lack balance in routing trust and energy efficiency. Trust-only routing achieves high routing reliability but sacrifices classification accuracy and generates higher violation rates. In contrast, the proposed STAD-MLTRS framework achieves a comprehensive improvement, combining superior detection metrics with minimal false positives, faster detection and mitigation times, lower SLA violations, higher routing trust, and reduced energy consumption. This demonstrates that the integration of multi-layer threat detection, temporal trust profiling, and secure routing enables the framework to outperform all baselines, providing a holistic solution for safeguarding IoT-enabled smart city infrastructures.

Figure 2 presents a comparative view of overall detection performance across different approaches. The results reveal that traditional signature-based intrusion detection lags behind, delivering the lowest composite score due to its dependence on predefined patterns and its limited adaptability to new or evolving threats. Classical machine learning methods such as Random Forest and SVM perform better, achieving moderate gains by recognizing statistical patterns, yet they remain constrained when faced with complex multi-stage intrusions. Advanced deep learning models, including BERT for email-based threats and LSTM for network traffic, demonstrate stronger capabilities with higher detection indices, reflecting their ability to capture contextual cues and temporal dependencies. Trust-only routing shows reliability in securing paths but falls short in comprehensive threat identification, which lowers its overall performance index. In contrast, the proposed STAD-MLTRS framework achieves the highest detection performance, demonstrating its effectiveness in combining contextual filtering, behavioral trust profiling, and anomaly-aware routing. This balanced integration allows it to isolate attacks more accurately and consistently, establishing it as the most reliable solution among all compared methods.

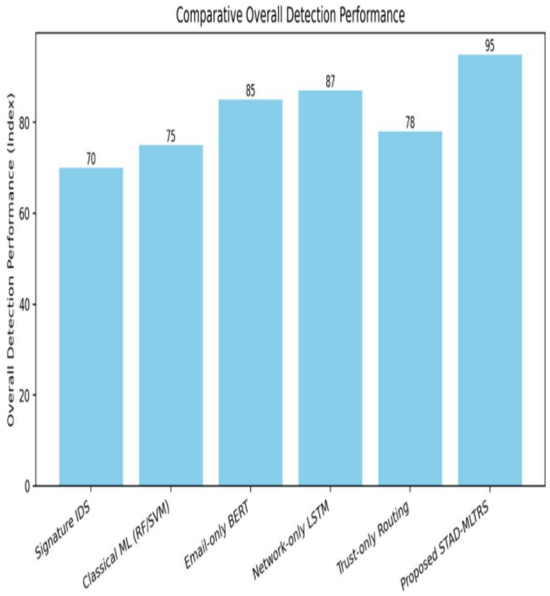

Figure 2: Comparative Overall Detection Performance

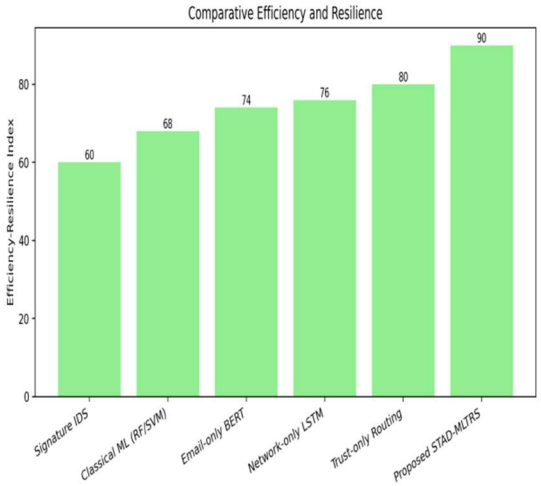

Figure 3: Comparative Efficiency and Resilience

Figure 3 compares the efficiency and resilience levels of the evaluated methods by combining routing trust, SLA compliance, and energy utilization into a single index. The results indicate that conventional signature-based IDS is the least effective, as it consumes more energy while offering weaker routing stability and higher SLA violations. Classical ML models improve efficiency somewhat but still struggle to provide consistent resilience in large-scale, heterogeneous IoT environments. Deep learning models such as BERT and LSTM achieve stronger resilience by improving routing trust and lowering violations, but their energy consumption remains relatively high, limiting sustainability. Trust-only routing demonstrates excellent path reliability and relatively low overhead; however, its narrow focus on routing makes it less effective in addressing broader security challenges. The proposed STAD-MLTRS framework delivers the best balance, achieving high routing trust, minimal SLA violations, and reduced energy consumption, resulting in the strongest efficiency–resilience index overall. This confirms that integrating multi-layer trust with adaptive threat detection creates a robust solution capable of supporting secure and sustainable operations in IoT-enabled smart cities.

The overall findings demonstrate that the proposed STAD-MLTRS framework consistently outperforms traditional IDS, classical machine learning, and standalone deep learning models across all critical dimensions of security and performance. By integrating contextual threat filtering, temporal trust profiling, and adaptive routing optimization, the framework achieves superior detection accuracy with minimal false positives, while also reducing detection and mitigation delays. At the same time, it enhances operational resilience by lowering SLA violations, increasing routing trust, and improving energy efficiency, ensuring a sustainable approach for large-scale IoT deployments. Unlike other methods that excel in isolated aspects such as routing reliability or anomaly classification, STAD-MLTRS delivers a balanced, end-to-end defense mechanism that safeguards both communication content and routing behavior. These results confirm its suitability for real-world smart city infrastructures, where scalability, adaptability, and sustainability are as important as high detection accuracy.

6. CONCLUSION

The proposed STAD-MLTRS framework delivers a comprehensive and adaptive security solution for IoT-enabled smart cities by integrating intelligent threat detection, temporal trust profiling, and dual-layer routing optimization. The evaluation results confirm its effectiveness, achieving 98.2% detection accuracy with a very low false positive rate of 1.7%, while also reducing SLA violations, lowering mean detection and mitigation times, and improving routing trust and energy efficiency. These outcomes demonstrate that STAD-MLTRS not only enhances security performance but also provides a balanced approach that ensures reliability, scalability, and sustainability in complex IoT ecosystems.

Looking forward, the framework can be extended to incorporate advanced mechanisms such as transfer learning and federated learning to further improve adaptability across heterogeneous domains without centralized data dependencies. Integrating blockchain-based trust models could enhance transparency and resilience in distributed environments, while real-time adaptive retraining and cross-domain intelligence sharing would strengthen defenses against zero-day exploits and multi-stage coordinated attacks. Moreover, energy-aware optimization will be essential to support deployment in resource-constrained edge devices, enabling sustainable operations. By advancing in these directions, STAD-MLTRS can evolve into a more robust foundation for securing smart cities, fostering digital trust, and ensuring the safe growth of next-generation urban infrastructures.

REFERENCES

[1]. Ahmed MR, Shatabda S, Islam AM, Robin MT. Intrusion Detection System in Software-Defined Networks Using Machine Learning

and Deep Learning Techniques--A Comprehensive Survey. Authorea Preprints. 2021.

[2]. Ferrão T, Manene F, Ajibesin AA. Multi-Attack Intrusion Detection System for Software-Defined Internet of Things Network. Computers, Materials & Continua. 2023 Jun 1;75(3).

[3]. Zainudin A, Ahakonye LA, Akter R, Kim DS, Lee JM. An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks. IEEE Internet of Things Journal. 2022 Aug 8;10(10):8491-504.

[4]. Elsayed RA, Hamada RA, Abdalla MI, Elsaid SA. Securing IoT and SDN systems using deep learning based automatic intrusion detection. Ain Shams Engineering Journal. 2023 Oct 1;14(10):102211.

[5]. Kumari P, Jain AK, Pal Y, Singh K, Singh A. Towards Detection of DDoS Attacks in IoT with Optimal Features Selection. Wireless Personal Communications. 2024 Jul;137(2):951-76.

[6]. Kavitha D, Ramalakshmi R. Machine learning-based DDOS Attack Detection and Mitigation in SDNs for IoT environments. Journal of the Franklin Institute. 2024 Nov 1;361(17):107197.

[7]. Dey AK, Gupta GP, Sahu SP. A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. Decision Analytics Journal. 2023 Jun 1; 7:100206.

[8]. Logeswari G, Bose S, Anitha TJ. An intrusion detection system for sdn using machine learning. Intelligent Automation & Soft Computing. 2023 Jan 1;35(1):867-80.

[9]. Alavizadeh H, Alavizadeh H, Jang-Jaccard J. Deep Q-learning based reinforcement learning approach for network intrusion detection. Computers. 2022 Mar 11;11(3):41.

[10]. Alenezi N, Aljuhani A. Intelligent Intrusion Detection for Industrial Internet of Things Using Clustering Techniques. Computer Systems Science & Engineering. 2023 Sep 1;46(3).

[11]. Michelena A, Aveleira-Mata J, Jove E, Bayón-Gutiérrez M, Novais P, Romero OF, Calvo-Rolle JL, Aláiz-Moretón H. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems. 2024 Feb;41(2): e13263.

[12]. Saheed YK, Usman AA, Sukat FD, Abdulrahman M. A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network. Frontiers in Computer Science. 2023 Apr 11; 5:997159.

[13]. Salvakkam DB, Saravanan V, Jain PK, Pamula R. Enhanced quantum-secure ensemble intrusion detection techniques for cloud based on deep learning. Cognitive Computation. 2023 Sep;15(5):1593-612.

[14]. Kasongo SM. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer Communications. 2023 Feb 1; 199:113-25.

[15]. El-Ghamry A, Darwish A, Hassanien AE. An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things. 2023 Jul 1; 22:100709.

[16]. Soleymanzadeh R, Aljasim M, Qadeer MW, Kashef R. Cyberattack and fraud detection using ensemble stacking. AI. 2022 Jan 18;3(1):22-36.

[17]. Zeeshan AL, Tiberti W, Marotta A, Cassioli D. Deep Transfer Learning for Intrusion Detection in Edge Computing Scenarios. IEEE Internet of Things Journal. 2025 Aug 11.

[18]. Heidari A, Navimipour NJ, Unal M. A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. IEEE Internet of Things Journal. 2023 Jan 20;10(10):8445-54.

[19]. Mukherjee I, Sahu NK, Sahana SK. Simulation and modelling for anomaly detection in IoT network using machine learning. International journal of wireless information networks. 2023 Jun;30(2):173-89.

[20]. Mehedi ST, Anwar A, Rahman Z, Ahmed K, Islam R. Dependable intrusion detection system for IoT: A deep transfer learning-based approach. IEEE Transactions on Industrial Informatics. 2022 Apr 5;19(1):1006-17.

[21]. Al-Hawawreh M, Sitnikova E, Aboutorab N. X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things. IEEE Internet of Things Journal. 2021 Aug 3;9(5):3962-77.

[22]. Zhou F, Yuan M, Liu Y, Zhang H, Gu M, Zhou T. Niect: A model for intrusion security detection applied to campus video surveillance edge networks. In2024 IEEE 11th International Conference on Cyber Security and Cloud Computing (CSCloud) 2024 Jun 28 (pp. 24-29). IEEE.

[23]. Hillier C, Karroubi T. Turning the hunted into the hunter via threat hunting: Life cycle, ecosystem, challenges and the great promise of AI. arXiv preprint arXiv:2204.11076. 2022 Apr 23.

[24]. Mahamat M, Jaber G, Bouabdallah A. Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges. Wireless networks. 2023 Feb;29(2):787-808.

[25]. Gyamfi E, Jurcut A. Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors. 2022 May 14;22(10):3744