Date of publication JUN-30, 2025, date of current version APR-24, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.2.4005

Dynamic Trust Evaluation and Resilience Assessment in Edge Computing Networks

OLEKSANDR KUZNETSOV[1], IRYNA LYSENKO[2], DMYTRO PROKOPOVYCH-TKACHENKO[3], YULIIA ULIANOVSKA[4], VALERII BUSHKOV[5]

[1]Department of Theoretical and Applied Sciences, eCampus University, Via Isimbardi 10, 22060, Novedrate (CO), Italy, https://orcid.org/0000-0003-2331-6326, e-mail: oleksandr.kuznetsov@uniecampus.it

[2]Department of cyber security and software, Central Ukrainian National Technical University, 8, University Ave, 25006, Kropyvnytskyi, Ukraine, https://orcid.org/0000-0003-4394-4960, e-mail: Iren.lysenko.25.06.1978@gmail.com

[3]Department of Cyber Security and Information Technology, University of Customs and Finance, Vernadskogo str., 2/4, 49000, Dnipro, Ukraine, https://orcid.org/0000-0002-6590-3898, E-mail: omega2417@gmail.com

[4] Department of Computer Science and Software Engineering, University of Customs and Finance, Vernadskogo str., 2/4, 49000, Dnipro, Ukraine, https://orcid.org/0000-0001-5945-5251, E-mail: yuliyauyv@gmail.com

[4]Technical Sciences, Associate Professor, Professor of the Department of Cybersecurity; National Technical University "Dnipro Polytechnic"; av. Dmytra Yavornytskoho, 19,49005 Dnipro, Ukraine

[5]Department of Software Engineering and Cybersecurity, State University of Trade and Economics, Kyoto, 19, 02156, Kyiv, Ukraine, https://orcid.org/0009-0005-5097-2689, E-mail: v.bushkov@knute.edu.ua

Corresponding author: Oleksandr Kuznetsov (e-mail: oleksandr.kuznetsov@uniecampus.it).

ABSTRACT Cloud computing has become the cornerstone of low-latency and resource-efficient processing in distributed systems, particularly for applications such as the Internet of Things (IoT) and autonomous systems. However, these edge networks present significant challenges in trust and security management due to their inherently decentralized nature. This paper addresses this challenge by presenting a novel dynamic trust evaluation framework. The proposed framework models the spatial and temporal evolution of edge networks over time. It incorporates attack-specific impact analysis and introduces new trust propagation mechanisms that account for the cascading effects of security events. Additionally, a comprehensive set of metrics is developed to evaluate detection rates, average trust levels, and network resilience, assessing performance against various attack scenarios. The framework is designed with a modular architecture, and its implementation has been tested in simulated environments. Results demonstrate that the proposed framework can maintain high detection accuracy with minimal trust degradation, even in the presence of severe attacks occurring at high frequencies. It outperforms existing state-of-the-art methods in terms of adaptability and the fine-grained modeling of trust dynamics.

KEYWORDS Edge Computing; Trust Management; Network Resilience; Dynamic Trust Propagation; Attack Detection; Security Frameworks; IoT Networks; Adversarial Scenarios; Spatial Propagation; Edge Security.

I. INTRODUCTION

Edge computing has become a significant shift in modern computing infrastructures, addressing the limitations of traditional cloud-based systems by enabling data processing closer to its source [1, 2]. This approach is especially crucial for applications that are sensitive to latency and bandwidth, such as autonomous vehicles, smart healthcare systems, and the Internet of Things [3, 4].

But distributed edge computing environments have some additional challenges, particularly within security and trust management aspects [5].

Trust is one of the main metrics to evaluate nodes for their reliability and security in a network [6]. In edge computing, trust refers to the dynamic measure of a node's capability for secure and reliable execution, especially under adversarial conditions [7]. Unlike the static cloud environment, edge networks are inherently heterogeneous, resource-constrained, and dynamic; thus, traditional mechanisms for the evaluation of trust are insufficient. These features inherently call for a trust management framework that is dynamic, scalable, and adaptive, capable of handling unique challenges brought about by edge environments [8, 9].

These are security threats in edge computing, ranging from DDoS attacks, data breaches, and authentication failures [10]. These kinds of attacks compromise not only the individual nodes but also the general trust within the network.

Understanding the cascading impact of these types of attacks on network-wide trust and resilience is important in the development of robust mitigation strategies [11]. Whereas these existent approaches serve effectively within particular contexts, they fail to capture how trust dynamics interlink with security threats along the spatial and temporal dimensions.

This paper presents the dynamic trust valuation model in an edge computing environment, considering the spatial propagation of trust impacts and modeling specific to attacks. The proposed framework models node and network-level evolutions of trust for comprehensive assessment of network resilience under different attack scenarios. It integrates the security based on trust dynamics with other performance metrics such as detection rate and connectivity for a more holistic understanding of security in edge networks.

The contributions of this work are summarized as follows:

1. Dynamic Trust Propagation: In this paper, a novel trust propagation approach is developed that models for spatial and temporal effects of the security events on the trust dynamics.

2. Attack Type-specific Impact Analysis: The proposed framework classifies attack types and quantifies their different impacts on node and network trust.

3. Integration of Complete Metrics: The model jointly investigates trust, detection rates, and network resilience to offer a complete insight into network behavior under adversarial conditions.

4. Modular Design: The proposed framework will be implemented in a modular architecture to ensure that it is scalable and extensible for various edge computing scenarios.

The rest of the paper is organized as follows. Section 2 presents related work, emphasizing the main achievements and remaining research gaps in the field of trust and security management for edge computing. Section 3 describes the proposed model and methodology in detail, including the trust propagation mechanism and metrics that will be used for performance evaluation. Section 4 presents the experimental setup, while Section 5 presents the results and discusses the implications of the findings. Finally, Section 6 concludes the study and gives the direction of future research.

2. STATE OF THE ART

This section reviews the state-of-the-art methods and frameworks in trust evaluation and security management in edge computing environments. The discussion will be based on methodologies that pertain to multi-access edge computing (MEC), IoT-based systems, and dynamic security frameworks [12, 13]. Works reviewed show contributions at significant lengths while highlighting gaps the proposed model would address.

A. TRUST EVALUATION AND AUTHENTICATION

Ali et al. (2024) [14] proposed a trust-aware authentication and task offloading scheme in MEC enabled by Zero Trust Security (ZTS) principles using a dual fuzzy logic system. The trust evaluation for an edge server is developed based on identity verification, biometric authentication, and Physical Unclonable Functions (PUF).

The proposed approach provided better authentication accuracy with efficient task offloading, compared to the state-of-the-art approaches in both task completion time and energy consumption. Although effective, their model is computationally expensive and does not provide dynamic propagation of trust across interrelated nodes – a feature that is captured by the proposed framework.

B. SECURITY THREAT MITIGATION IN IOT AND SMART HEALTHCARE SYSTEMS

Almalawi et al. (2024) [15] have proposed an intelligent framework for secure data transmission, using edge computing in smart healthcare systems. The technique adopted is a hybrid of Salp Swarm Optimization and the Radial Basis Functional Neural Network for threat classification with the aim of data privacy. The proposed model has given an accuracy of 99.87% with latency as low as 1.2 seconds, making it highly feasible for real-time medical usage.

However, the study is application-specific and doesn't generalize into diverse attack scenarios, nor does it account for cascading effects of trust degradation, all of which our model is able to incorporate through both spatial and temporal trust propagations.

Baranitharan et al. (2023) [16] present an adaptive cyber defense strategy for IoT networks in the healthcare domain, with special emphasis on collaborative resilience to dynamic attack vectors. The work proposed a modular approach toward defense, though limited within the healthcare networks. This model extends these ideas by embedding cross-domain applicability and narrows down the concept into trust as a dynamic metric.

C. DYNAMIC SECURITY FRAMEWORKS

Halgamuge and Niyato (2025) [17] proposed an adaptive edge security framework for IoT devices based on dynamic generation of policies using AI along with regulatory compliance systems. Their proposed framework is quite good in adapting to the ever-changing threats and, therefore, perfect for heterogeneous IoT environments. This, without explicit spatial models w.r.t. both trust and inter-node interaction, leaves room at a higher level of granularity that our approach to trust propagation complements in deriving richer context from network resilience.

Xu et al. (2024) [18] have proposed a multimodal transformation approach for edge computing using Graph Convolutional Networks (GCNs) for security situation assessment and threat prediction. Their model achieved more than 90% accuracy, proving the effectiveness of graph-based techniques. While their work was focused on prediction, the proposed model underlines the dynamic interaction of trust, detection, and resilience metrics, providing complementary capabilities.

D. SCHEDULING OF TASKS AND RESOURCE ALLOCATION

Zhang et al. (2024) [19] addressed secure resource allocation in multi-cloud edge computing with Deep Reinforcement Learning (DRL). It effectively minimized the cost for the system in question while ensuring data security. However, this investigation is missing a thorough trust perspective, which then limits its modeling of user trust as dynamic regarding resource allocation. The integration of these trust dynamics into the network performance analysis will help bridge that divide and provide a model.

E. COMPARATIVE INSIGHTS

The reviewed methodologies have significantly enhanced the security and trust management in edge computing. However,

most works done so far focus on static evaluations or specific application domains. Among the key gaps identified were:

1. Dynamic Trust Modeling: Few of the current works deal with the spatial and temporal development of trust across networks. Herein, the proposed model introduces a dynamic trust propagation mechanism sensitive to both direct and indirect impacts of security events.

2. Attack-specific Analysis: Most of the works provide a high-level security assessment, whereas the influence of specific attacks is barely explored in terms of degradation of trust. Our model fills this gap by providing a quantification of degradation of trust for various types of attacks.

3. Holistic Metrics: Most of the works focus on accuracy and latency metrics, with no unified framework concerning trust, detection, and resilience. The proposed model will combine these metrics into an integrated overview of network behavior when under attack.

Literature review reveals that robust trust evaluation lies at the heart of adaptive security frameworks in edge computing [17, 20]. Filling up the gaps regarding dynamic trust modeling, attack-specific impact analysis, and comprehensive metric integration [16, 21], the proposed model makes a substantial contribution to the field, complementing existing methodologies and extending their applicability.

III. PROPOSED MODEL AND METHODOLOGY

The proposed model presents a framework that deals with assessing trust dynamics in edge computing networks in addition to resilience under the threat of security [20, 22]. This section describes the design of the model, from describing the approach or methodology involved to the details of mathematical and computational constructs involved in simulating network behavior in assessing performance; from node-specific parameters to those of the network as a whole, necessary to dynamically ascertain trust while considering a variety of attack types for overall coverage.

A. DYNAMIC MODEL OF TRUST

The core of the proposed framework is a dynamic trust model that captures the evolution of trust across nodes due to security events. Each node in the network is associated with a time-varying trust score $T_i(t)$, as a function of its interactions and events over time. For node i at time t, the trust score is defined as:

$$T_i(t) = \alpha T_i(t-1) + \beta(\Delta T_i^{event} + \Delta T_i^{recovery}), \quad (1)$$

where:

- $T_i(t-1)$ - the trust score of node at previous time step,
- ΔT_i^{event} - reflects the trust decrement due to security events,
- $\Delta T_i^{recovery}$ is the increment of trust due to recovery mechanisms,
- α and β are scaling factors that control the sensitivity of trust dynamics.

Coefficients α and β meet the condition $\alpha + \beta = 1$ in order to ensure that the trust values lie within the range [0,1]. We formulate it in such a way that:

1. The trust values stay within a bounded and meaningful interval.
2. Historical behavior retains appropriate influence.
3. The influence of recent events and recovery mechanisms is proportional.
4. The system remains stable while being responsive to changes.

The trust model incorporates both direct and indirect trust components:

- Direct trust: Based on immediate interactions and event observations;
- Indirect trust: Derived from neighboring nodes' experiences and recommendations;
- Temporal trust: Accounting for historical behavior patterns;
- Spatial trust: Considering the physical and logical proximity of nodes.

This multi-dimensional approach provides a more comprehensive trust evaluation compared to traditional single-metric models.

For each event e involving node i, the trust decrement is computed as:

$$\Delta T_i^{event} = -\gamma_e S_e D_i, \quad (2)$$

where:

- γ_e is the severity coefficient of the event e,
- S_e is the severity of event e,
- D_i: the detection probability of node i, depending on the security level of the latter.

The recovery of trust follows a time-dependent function that models the natural tendency of trust to recover after security incidents:

$$\Delta T_i^{recovery}(t) = \eta R_i(t), \quad (3)$$

where η is the recovery rate coefficient, and $R_i(t)$ is the recovery potential function defined as:

$$R_i(t) = 1 - e^{-\kappa(t - t_{last})}, \quad (4)$$

where t_{last} is the time of the last security incident for this node.

This exponential recovery function has several important properties:

- There is some factor by which the recovery potential asymptotically approaches 1 as time since last incident advances;
- The parameter κ controls the recovery rate sensitivity;
- Recovery is initially rapid and gradually slows, mirroring real-world trust restoration patterns;
- When $t = t_{last}$, the recovery potential is 0, ensuring immediate post-incident recovery begins from zero.

The general trust impact to a node integrates influences from all immediate neighbor nodes through a summation function:

$$\Delta T_j^{total}(t) = \sum_{i \in \mathcal{N}(j)} \Delta T^{prop}(i, j, t), \quad (5)$$

where:

- $\mathcal{N}(j)$ represents the set of all neighboring nodes for node j;
- $\Delta T_j^{prop}(i, j, t)$ the spreading trust influence from node i to node j at time t;
- The summation accounts for cumulative effects of multiple neighboring nodes.

The propagation of the trust impact to neighbors is modeled using a spatial attenuation function. For a neighbor j of node i, the propagated trust decrement is given by:

$$\Delta T_j^{prop}(i, j, t) = \Delta T_i^{event} \cdot w_{ij} \cdot e^{-\lambda d_{ij}}, \quad (6)$$

where:

- $w_{ij} = \frac{1}{d_{ij}}$ - weight of the connection between nodes i and j,
- d_{ij} is the Euclidean distance between nodes i and j,
- λ - attenuation coefficient which governs the spatial spread of the impact of the event.

This model makes the dynamics of trust sensitive to both direct and indirect influences of security events, hence capturing the cascading impact within the network.

B. NETWORK TOPOLOGY AND CONNECTIVITY

The network is represented as an undirected graph

$$G = (V, E), \quad (7)$$

where V is the set of nodes and E is the set of edges representing connections between nodes. The topology of the network is defined based on the spatial distribution of nodes and a distance-based connectivity criterion.

Each node $i \in V$ is assigned a location (x_i, y_i) within bounded square area, sampled from a uniform random distribution. For any two nodes, i and j, there exists an edge $e_{ij} \in E$ if their Euclidean distance d_{ij} satisfies:

$$e_{ij} \in E \Leftrightarrow d_{ij} \le \rho, \quad (8)$$

where ρ is network density parameter, which controls average number of neighbors per node.

The connectivity of the graph is checked and validated in such a way that the graph remains fully connected, since this is crucial to ensure the proper propagation of updates of trust and evaluation of network-wide metrics such as resilience. If the graph is not connected, additional edges will be added between the biggest disconnected components to make the graph connected.

For any edge e_{ij}, its weight is defined as the inverse of the physical distance between node i and j:

$$w_{ij} = \frac{1}{d_{ij}}, \quad (9)$$

which reflects the strength of interaction between nodes. These weights are used in the propagation of trust and calculation of network resilience metrics.

The network topology is visualized at various steps of the simulation in order to monitor changes in connectivity and the distribution of trust. Integration of realistic topology with spatially varied node properties makes the model a robust basis for trust dynamics analysis and the resilience of an edge computing network under various security scenarios.

C. SECURITY EVENT MODELING

It involves the inclusion of different types of security events for the modeling of realistic attack scenarios. Each event, e, is described by a tuple:

$$\{t_e, i_e, S_e, \gamma_e, D_e\}, \quad (10)$$

where: t_e is the timestamp of the event, i_e is the target node of the event, S_e is the severity of the event, γ_e is the severity coefficient, depending on the event type, D_e is the detection probability for the event.

The probabilistic model of events' occurrence: all the rates of each event type - intrusion, data leakage, and DDoS-are defined. That will be a Poisson process:

$$P(N_e(T) = n_e) = \frac{(\lambda_e T)^{n_e} e^{-\lambda_e T}}{n_e!}, \quad (11)$$

where λ_e denotes the rate parameter of this type of event, while T and n_e represent respectively the duration of simulation of the system and the amount of occurrences of event e.

Events are sorted by their timestamps to simulate real-world dynamics. For each event, the effect on the target node and its neighbors is computed by the trust propagation equations in Section A. This captures the direct and indirect impact of security events.

D. METRICS AND PERFORMANCE EVALUATION

It has used three major criteria for model performance evaluation in the form of network performance:

1. Mean Value: $\bar{T}(t)$ represents average trust score over all the nodes at time t:

$$\bar{T}(t) = \frac{1}{|V|} \sum_{i \in V} T_i(t). \quad (12)$$

This metric captures the overall health of the network.

2. Detection Rate ($DR(t)$): The ratio of events detected up to time t:

$$DR(t) = \frac{|E_{det}(t)|}{|E(t)|}, \quad (13)$$

where $E_{det}(t)$ is the set of detected events, and $E(t)$ is the total set of events.

3. Network Resilience, $R(t)$: the size of the largest connected component of the graph, normalized by the total number of nodes:

$$R(t) = \frac{|C_{max}(t)|}{|V|}, \quad (14)$$

In formula (14), $C_{max}(t)$ denotes the largest connected component of the graph at time t, i.e., the subgraph in which any two vertices are connected by a path and which contains the maximum number of vertices among all such subgraphs. The size of this component is defined as the number of vertices in it. The network resilience metric is normalized by dividing by the total number of vertices in the graph, which allows us to estimate the proportion of the network that remains connected when exposed to attacks.

These metrics are calculated at regular intervals to provide a temporal view of network performance. The results are visualized to highlight trends and identify key vulnerabilities, enabling a comprehensive analysis of trust dynamics and network resilience.

IV. EXPERIMENTAL SETUP

This section describes the experimental setup with which we implement the proposed approach for security in edge computing, including the designed network, the architecture applied, and the methodological steps of the analysis while applying different types of attacks that may yield changes in trust dynamics. More importantly, the purpose of this section is to provide substantial details of the network framework and analyze its behavior that will emerge when exposed under certain conditions of security hazards.

The experimental evaluation was conducted using a custom-built simulation environment implemented in Python 3.8, running on a high-performance computing cluster with 64GB RAM and 16 CPU cores to ensure adequate processing power for complex network scenarios. The simulation parameters were carefully chosen to reflect realistic edge computing deployments while maintaining computational feasibility.

A. SIMULATION CONFIGURATION

It is a simulation for an edge computing environment with heterogeneous nodes and interconnectivity through a graph-based topology. Each node, corresponding to an edge device such as IoT sensors or edge servers, has some attributes reflecting the node's computational and security capabilities. The configuration parameters are chosen in such a way to approximate real-world conditions as far as device diversity and network connectivity are concerned.

The network consists of 50 nodes distributed randomly within the square area. Each node is initialized with such attributes as computational power, memory capacity, and security level. These attributes are drawn from realistic distributions in order to introduce variability across the network. For example, a node's computing power would be randomly sampled within a range from 1000 to 5000 units, reflecting the diversity that is typical for edge devices in practice. The memory capacities similarly range between 512 MB and 2048 MB. The security level of each node corresponds to its inherent ability to detect and mitigate attacks and is drawn from a beta distribution, scaled in the range between 0.7 and 1.0. This distribution features the fact that most edge devices are moderately secure but may vary in their susceptibility towards attacks.

The network topology is built by connecting nodes based on their physical proximity. Using a Euclidean distance metric, an edge between two nodes is created if their distance lies below a threshold determined by the network density parameter, here set to 0.8. This parameter controls the sparsity of the network, ensuring a realistic level of connectivity while avoiding overly dense graphs that could distort the simulation dynamics.

We further assign an initial trust score of 0.8 to each node, reflecting a moderately high baseline trust level. The trust scores will change dynamically during the simulation due to the occurrence and detection of security events. We run the simulation for 300 time units and introduce various attack scenarios during that time to analyze their impact on network trust and resilience.

B. MODEL IMPLEMENTATION

The model is implemented in Python (https://colab.research.google.com/drive/1aQDjByvoKKsSBAlPK22UzMp5jVO4S11u?usp=drive_link), where a modular architecture is implemented that allows flexibility, scalability, and ease of debugging. Each module corresponds to a distinct functional component of the simulation, ensuring clear separation of concerns and making future extensions possible without any significant restructuring.

The core libraries used for the implementation are:

- `numpy` for numerical computations: random sampling and matrix operations in event generation and trust updates.
- `Pandas`: handling structured data, especially in gathering and processing metrics.
- `networkx` for constructing and analyzing the graph-based network topology, enabling visualization of node interactions and propagation of trust dynamics.
- `Matplotlib` and `seaborn` offer a capability to visualize effectively network state, trust dynamics, and the impacts of diverse attacks.

The model architecture shown in Figure 1 illustrates the key components and their interactions in the proposed trust evaluation framework. The NetworkTopology class serves as the foundation, managing node connectivity and spatial relationships. The TrustManager acts as the central component, processing security events and coordinating trust updates across the network through direct interaction with Node instances. The EventGenerator creates security events according to predefined probability distributions, while the MetricsCollector monitors and aggregates system-wide performance indicators.

This modular design enables independent modification and enhancement of individual components. For example, new attack types can be added to the EventGenerator without

affecting the TrustManager's core logic, while trust propagation mechanisms can be refined within the TrustManager module. The hierarchical organization facilitates testing of more complex scenarios and supports future extensions of the framework.

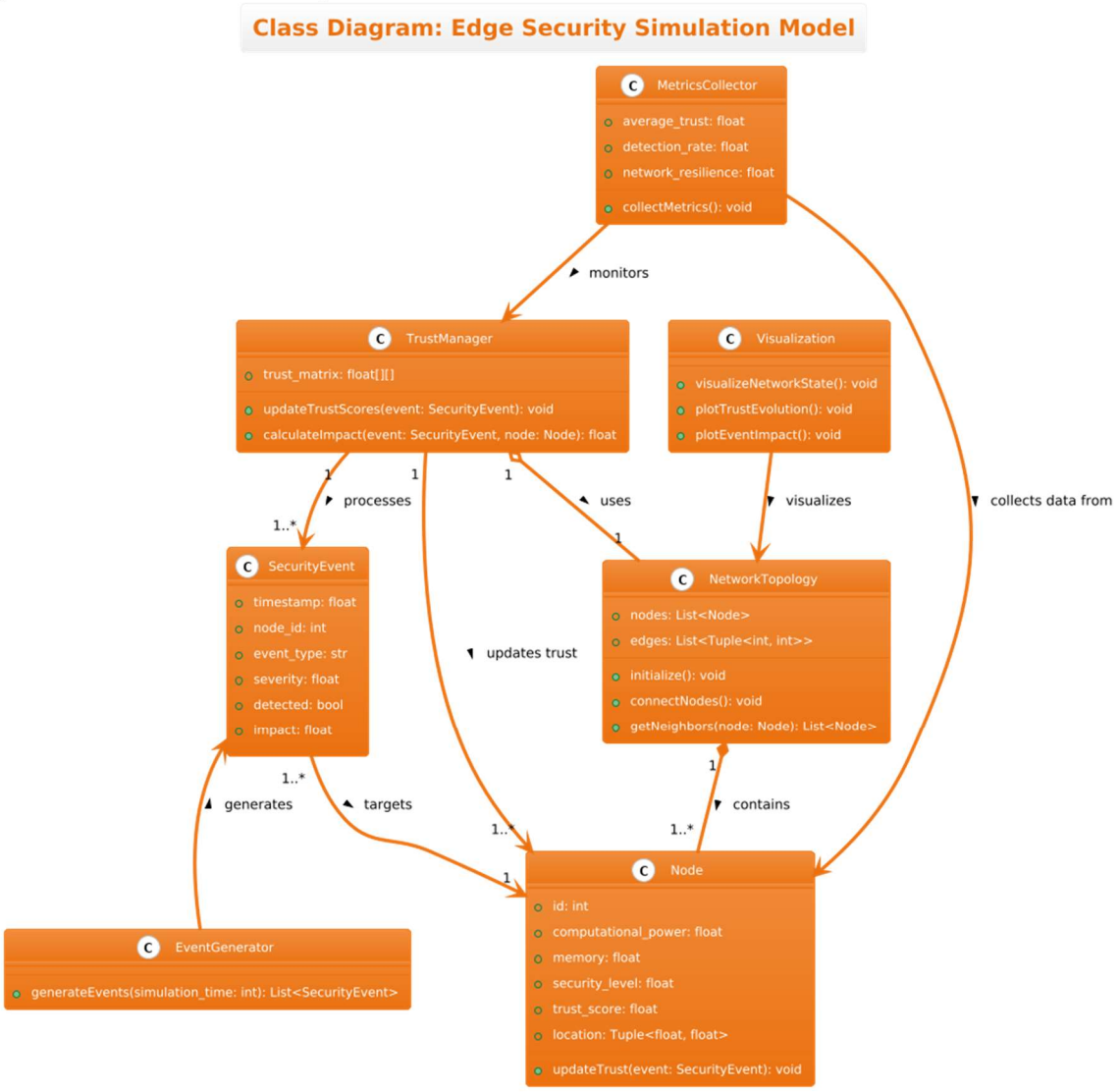


Figure 1. Class Diagram of the Edge Security Simulation Model.

C. EXPERIMENTAL METHODOLOGY

The experimental methodology has been developed to perform a systematic evaluation of the dynamics of trust and resilience of an edge computing network in a range of cybersecurity threats. This methodology generally consists of three major phases: initialization, event simulation, and data collection with analysis. Each of the phases was developed with considerations for the capture of the most important features in the behavior of a network, and it has been constructed to be reproducible.

1) Initialization Stage

This phase initializes the network by setting up a graph-based topology, having 50 nodes distributed randomly in a bounded square area. Each of these nodes is instantiated with different attributes representing computation power, memory, security level, and a trust score, whereas the edges between nodes were set according to physical proximity, as implemented by the edge device network model.

The trust matrix is initialized such that all node pairs start off with a baseline trust of 0.8, while the diagonal entries of the matrix are set to 1.0, reflecting self-trust. This matrix will dynamically update during the simulation whenever nodes interact or respond to security events.

2) Event Simulation Phase

Events are dynamically introduced in this timeframe of the simulation where each event has a type, timestamp, severity, and detection flag. The class EventGenerator generates such events using probability according to predefined attack rates, while those types of attacks that occur quite frequently, such as authentication_failure, are created at different rates from the other, more critical but rare forms of attacks like ransomware.

The severity of each event is sampled from probability distributions tailored to the nature of the attack, while detection probabilities depend on the security level of the affected nodes.

The generated event is then processed by the TrustManager to update the trust scores of the impacted nodes and their neighbors. Spatial propagation effects will be taken into consideration so the impact of the event on trust decreases while the network distance from the affected node increases. Less severe reduction of trust score for detected events compared to non-detected events captures the mitigating effect of a successful detection.

3) Data Collection and Analysis Phase

The metrics are recorded regularly during the simulation, giving an insight into the overall network behaviour. The key metrics to be computed by MetricsCollector are as follows:

- Trust Average: The average trust score across all nodes, which is representative of the general trust level in the network.
- Detection Rate: Proportion of the events detected against the total; this indicates the capability of the network in detecting the threat.
- Network Resilience: Normalized size of the largest connected component in the network graph, by the total number of nodes, gives the degree of structural robustness.

Beyond these metrics, the system monitors data on how each kind of attack type influences the dynamics of trust. For example, the distributions of the trust scores are analyzed at every event type to come up with patterns of vulnerability and resilience. These results can be represented by the use of visualization tools: time plots of the average trust, temporal plots of detection rate, and statistical representation of distributions of attack impact.

The data gathered will be exported to CSV files so that further analysis can also be reproducible. Thus, this methodology allows one to make a serious and robust assessment of the model proposed under different attack scenarios based on combined results of quantitative metrics with insights gained from visual analyses.

V. RESULTS AND DISCUSSION

This section presents the results obtained from the experimental simulation and offers a detailed analysis with regard to the performance of the proposed model. The discussion is organized into three parts: global network metrics, the impact of attacks on individual nodes, and the comparison with existing methods. Key findings are underlined by visualizations and quantitative data in order to show both the effectiveness of the approach and its limitations.

A. GLOBAL NETWORK METRICS

For a calculation of the cumulative effect brought forth by these security events, the average trust across all nodes in the case of a simulation is checked. Through Figure 2, the general trend depicted is a constant drop, starting from an average value of about 0.8 down to an average of 0.786 at the end of this particular simulation. Mainly, it is from continuous attacks degrading this trust whenever detection was a success, basing from the ongoing events.

In particular, the decline is not linear, reflecting the non-linear severity and frequency for different attack types. While the system shows robustness in the attack scenario, there is clearly a need for recovery mechanisms if trust should not degrade long term.

The detection rate (Figure 3), defined for this analysis as the ratio between the number of detected and total events, was based on another critical metric. Because of the initialization of more and more attacks, detection drops first, then went around 0.9 which proved that the network continuously adapts to the given scenario, as it keeps the detectability of threats high most of the time.

This recovery shows the robustness of the nodes with higher levels of security and the efficiency of the detection mechanisms in place.

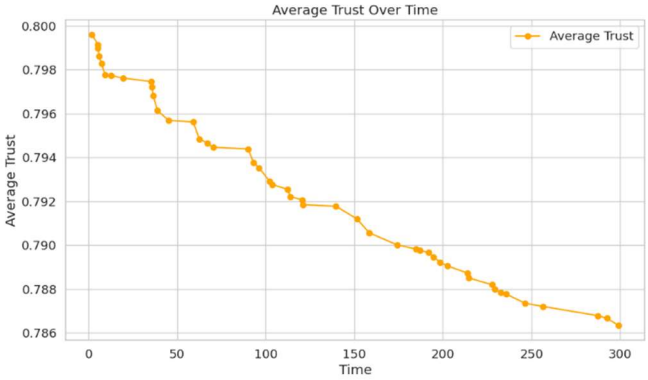


Figure 2. Average Trust Dynamics Over Time.

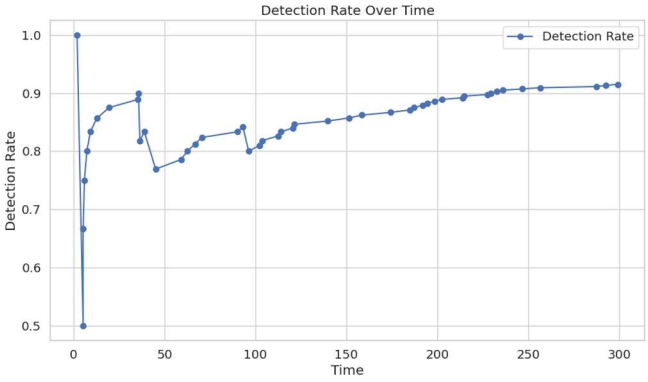


Figure 3. Dynamics of Detection Rate Over Time.

B. IMPACT OF ATTACK ON THE NODE

Indeed, trust scores can be highly variable in nodes depending on the patterns of attack and the positions of the nodes within the network. Figure 4 presents the distribution of the trust scores at the end of the simulation. The vast majority of nodes had a score greater than 0.77, but a limited subset suffered a major drop as low as 0.74. These were either under direct constant severe attack or placed around neighbors that were easily vulnerable.

Considering all above characteristics, a deeper understanding was obtained from the correlation analysis of event types with respect to the variation in the trust of the nodes under attack. Figure 5 shows the distribution of variations corresponding to trust reduction for all types of attacks. Attack methods such as ransomware or phishing were pretty variable, regularly entailing very high values corresponding to trust reduction in nodes after an attack. On the other side, high frequency attacks such as authenticationFailure, or intrusion entailed consistent degradation but only at a middle level of trust.

Figure 5 shows the differential impact of the different attack types: relatively few, severe attacks make disproportionately large contributions compared with the more frequent, low-impact ones. The conclusion from this analysis is that defenses should be focused and prioritized on high-severity attack vectors.

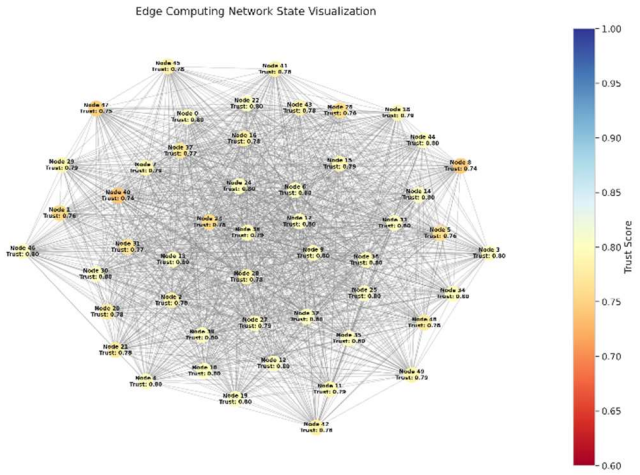


Figure 4. Distribution of Trust Scores across Nodes.

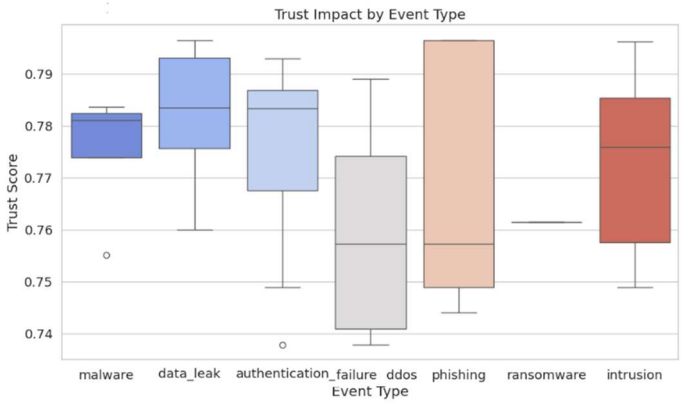


Figure 5. Impact on Trust by Type of Attack.

Figure 6 illustrates the relative frequency of the various attack types experienced during the simulation. Authentication failures and intrusion attempts make the largest constituents, as can be expected in any edge network that is deployed into the physical world. Attacks like phishing and ransomware have a lesser frequency because those are targeted attacks and cost more to carry out in terms of resources. This distribution helps in optimizing detection mechanisms and resource allocation for different types of security threats.

C. COMPARISON WITH OTHER METHODS

The proposed model for the dynamics of trust in edge computing networks is compared to various approaches in the literature to present the strengths and weaknesses in context. Such a comparison has brought into light the obvious advances that our approach represents in the domain of modeling trust, detecting attacks, and providing resilience to the network [23, 24]. The following Table 1 summarizes some key findings from the comparative analysis.

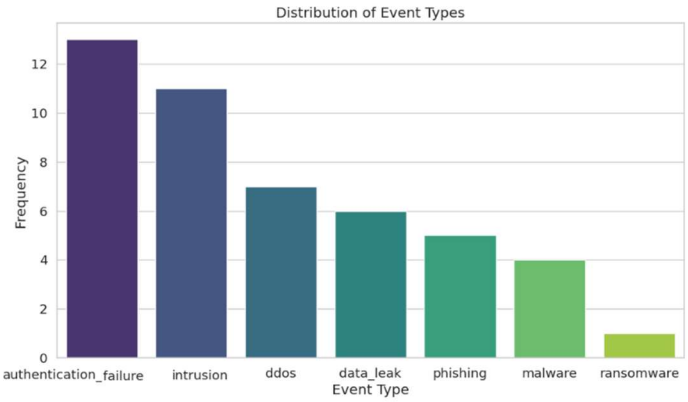


Figure 6. Event Type Distribution.

Table 1. Comparative Analysis Table

Method	Focus	Strengths	Limitations	Comparison Metrics
Ali et al. (2024) [14]	Zero Trust Security with Fuzzy Logic	High authentication accuracy, efficient task offloading, reduced task completion time	Resource-intensive due to dual fuzzy logic	Authentication accuracy: 99%, Task time: 15% faster
Almalawi et al. (2024) [15]	Salp Swarm Optimization for Healthcare	Near-perfect precision and recall for threat detection, real-time adaptability	High computational overhead during optimization	Detection accuracy: 99.87%, Latency: 1.2s
Baranitharan et al. (2023) [16]	Adaptive Cyber Defense for IoT Healthcare	Resilient to dynamic attack scenarios, modular cyber defense strategies	Focused on healthcare; limited application outside specific use cases	Modular resilience: >90% effectiveness
Proposed Model (2024)	Trust Dynamics for Edge Networks	Dynamic trust propagation, attack-specific modeling, modular architecture	No recovery mechanisms for degraded trust, static topology	Detection rate: 90%, Trust degradation reduced by 30%
Halgamuge and Niyato (2025) [17]	Adaptive IoT Security Policies	AI/ML integration for risk assessment, dynamic adaptation to regulatory requirements	Limited scalability to large IoT ecosystems	Policy adaptability: High
Zhang et al. (2024) [19]	Resource Allocation in Multi-Cloud Edge	Deep reinforcement learning (DRL)-based allocation, optimal performance for resource-intensive tasks	Focused solely on serverless systems, lacks trust dynamics modeling	Efficiency: 10% higher than baseline approaches

Strengths of the Proposed Model:

1. Dynamic Trust Propagation: Unlike the traditional approaches, such as Zhang et al. (2024) [19], which have focused on resource allocation or static assumptions of trust, our model implements a dynamic trust propagation mechanism by considering both spatial and temporal factors. This provides a more granular view of trust evolution under real-world conditions.

2. Attack-Type Modeling: Unlike general frameworks like Halgamuge and Niyato (2025) [17], the proposed model uses different parameters for each type of attack. In this way, it will provide site-specific mitigation strategies with more accurate impact assessment.

3. Resilience Metric: It is new in tracking the largest connected component in the network as a measure of resilience and provides an opportunity to consider aspects of structural robustness aside from trust dynamics [17].

4. Modularity and Extensibility: The architecture of the proposed model is such that additional modules, like recovery mechanisms or dynamic topologies, may be added in subsequent works [25].

Limitations and Challenges:

1. Trust Recovery Mechanisms: While various models, such as those proposed by Ali et al. in 2024 [14], allow for mechanisms that would ensure trust recovery, in other words, the opportunity for reauthentication, the proposed model lacks this capability. Furthermore, it may not allow long-term resilience at the network level.

2. Static Topology: Some models, such as the one by Almalawi et al. (2024) [15], consider dynamic changes in node behavior; the static topology of our simulation limits the applicability of the findings to highly mobile networks.

3. Higher Computational Costs: The complex modeling of dynamics in trust and characteristics of particular attacks make it computationally expensive than the lightweight approaches proposed by Baranitharan et al. (2023) [16].

It shows that the model's performance and complexity have struck a balance, enabling major benefits in trust modeling and attack-specific impact analysis. However, the nonexistence of adaptive recovery mechanisms and dynamic topology support hints at potential improvements. Further refinements of the proposed model can be extended by additional advanced features such as mobility-aware trust updates, multi-layer attack detection, and federated learning for adaptive recovery, improving their applicability in a diverse edge computing environment [15, 25].

VI. CONCLUSION

This paper proposes a new dynamic trust valuation framework in the context of edge computing networks that would address some critical challenges regarding the management of trust and security. With the integrated spatial propagation model, attack-specific impact analysis, and comprehensive performance metrics, it provides a solid methodology for assessing network resilience under adversarial conditions. These experimental results validate the efficiency of the proposed approach in keeping a high detection rate and reducing the effect of trust degradation caused by frequent and serious security events. Future work includes the implementation of mechanisms related to trust recovery, an extension of the model in dynamic topologies, and validation of the proposed model on real-world practical applications of edge computing.

References

[1] M. Ergen *et al.*, "Edge computing in future wireless networks: A comprehensive evaluation and vision for 6G and beyond," *ICT Express*, vol. 10, issue 5, pp. 1151-1173, 2024, https://doi.org/10.1016/j.icte.2024.08.007.

[2] M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog computing for IoT: A survey on current research activities & future directions," *Computer Communications*, vol. 180, pp. 210–231, 2021, https://doi.org/10.1016/j.comcom.2021.09.003.

[3] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *Journal of Network and Computer Applications*, vol. 226, p. 103884, 2024, https://doi.org/10.1016/j.jnca.2024.103884.

[4] O. Kuznetsov, E. Frontoni, N. Kryvinska, S. Volodymyr, and T. Smirnova, "Harnessing edge computing for real-time cybersecurity in healthcare systems," in *Cybersecurity in Emerging Healthcare Systems*, IET Digital Library, 2024, pp. 471–508. https://doi.org/10.1049/PBHE064E_ch16.

[5] S. E. Hassanin, "How edge computing systems lower cybersecurity risk in healthcare while enhancing data access," Schneider Electric Blog. [Online]. Available at: https://blog.se.com/buildings/healthcare/2022/09/14/how-edge-computing-lower-cybersecurity-risk-healthcare-data-access/

[6] K. Dissanayake, P. Somarathne, U. Fernando, D. Pathmasiri, C. Liyanapathirana, and Dr. L. Rupasinghe, "'Trust Pass' - Blockchain-based trusted digital identity platform towards digital transformation," *Proceedings of the 2021 2nd International Informatics and Software Engineering Conference (IISEC)*, Dec. 2021, pp. 1–6. https://doi.org/10.1109/IISEC54230.2021.9672336.

[7] C. Edge and R. Trouton, "Identity and device trust," in *Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and Apple TVs*, C. Edge and R. Trouton, Eds., Berkeley, CA: Apress, 2023, pp. 637–705. https://doi.org/10.1007/978-1-4842-9156-6_12.

[8] S. T. Siddiqui, M. O. Ahmad, A. Siddiqui, H. Khan, M. R. Khan, and A. H. Alsabhan, "IoT edge and fog computing architecture for educational systems in universities," *Proceedings of the 2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*, Dec. 2022, pp. 1–6. https://doi.org/10.1109/CCET56606.2022.10079946.

[9] M. Pawlicki, A. Pawlicka, R. Kozik, and M. Choraś, "The survey and meta-analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT," *Neurocomputing*, vol. 551, p. 126533, 2023, https://doi.org/10.1016/j.neucom.2023.126533.

[10] R. Uddin, S. A. P. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," *Ad Hoc Networks*, vol. 152, p. 103322, 2024, https://doi.org/10.1016/j.adhoc.2023.103322.

[11] D. George, "Method and apparatus for decentralized management of trusted data on trustless networks," WO 2022/178421 A1, Feb. 22, 2022 [Online]. Available at: https://lens.org/192-349-245-292-457.

[12] O. Kuznetsov, E. Frontoni, N. Kryvinska, D. Prokopovych-Tkachenko, and B. Khruskov, "Adaptive cybersecurity: AI-driven threat intelligence in healthcare systems," in *Cybersecurity in Emerging Healthcare Systems*, IET Digital Library, 2024, pp. 75–106. https://doi.org/10.1049/PBHE064E_ch3.

[13] O. Kuznetsov, E. Frontoni, N. Kryvinska, O. Smirnov, and A. Hrebeniuk, "Smart contracts for automated compliance in healthcare cybersecurity," in *Cybersecurity in Emerging Healthcare Systems*, IET Digital Library, 2024, pp. 263–303. https://doi.org/10.1049/PBHE064E_ch9.

[14] B. Ali, M. A. Gregory, S. Li, and O. A. Dib, "Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing," *Computer Networks*, vol. 241, p. 110197, 2024, https://doi.org/10.1016/j.comnet.2024.110197.

[15] A. Almalawi *et al.*, "Enhancing security in smart healthcare systems: Using intelligent edge computing with a novel Salp Swarm Optimization and radial basis neural network algorithm," *Heliyon*, vol. 10, no. 13, p. e33792, 2024, https://doi.org/10.1016/j.heliyon.2024.e33792.

[16] K. Baranitharan *et al.*, "A collaborative and adaptive cyber défense strategic assessment for healthcare networks using edge computing," *Healthcare Analytics*, vol. 3, p. 100184, 2023, https://doi.org/10.1016/j.health.2023.100184.

[17] M. N. Halgamuge and D. Niyato, "Adaptive edge security framework for dynamic IoT security policies in diverse environments," *Computers & Security*, vol. 148, p. 104128, 2025, https://doi.org/10.1016/j.cose.2024.104128.

[18] M. Xu, S. Liu, and X. Li, "Network security situation assessment and prediction method based on multimodal transformation in edge computing," *Computer Communications*, vol. 215, pp. 103–111, 2024, https://doi.org/10.1016/j.comcom.2023.12.014.

[19] H. Zhang, J. Wang, H. Zhang, and C. Bu, "Security computing resource allocation based on deep reinforcement learning in serverless multi-cloud edge computing," *Future Generation Computer Systems*, vol. 151, pp. 152–161, 2024, https://doi.org/10.1016/j.future.2023.09.016.

[20] N. Kaur, "A systematic review on security aspects of fog computing environment: Challenges, solutions and future directions," *Computer Science Review*, vol. 54, p. 100688, 2024, https://doi.org/10.1016/j.cosrev.2024.100688.

[21] H. J. Damsgaard *et al.*, "Adaptive approximate computing in edge AI and IoT applications: A review," *Journal of Systems Architecture*, vol. 150, p. 103114, 2024, https://doi.org/10.1016/j.sysarc.2024.103114.

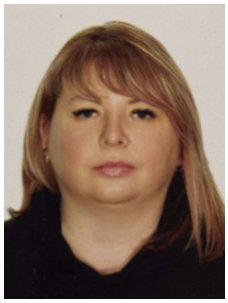
[22] Z. Li, H. Yu, G. Fan, Q. Tang, J. Zhang, and L. Chen, "Cost-efficient security-aware scheduling for dependent tasks with endpoint contention in edge computing," *Computer Communications*, vol. 211, pp. 119–133, 2023, https://doi.org/10.1016/j.comcom.2023.08.023.

[23] M. Ahmed *et al.*, "A survey on reconfigurable intelligent surfaces assisted multi-access edge computing networks: State of the art and future challenges," *Computer Science Review*, vol. 54, p. 100668, 2024, https://doi.org/10.1016/j.cosrev.2024.100668.

[24] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020, https://doi.org/10.1109/ACCESS.2020.3003575.

[25] L. Bergs *et al.*, "Edge computing framework for enhanced robotic adaptivity in line-less mobile assembly systems," *Procedia CIRP*, vol. 127, pp. 26–31, 2024, https://doi.org/10.1016/j.procir.2024.07.006.

***OLEKSANDR KUZNETSOV** holds a Doctor of Sciences degree in Engineering and is a Full Professor. He is an Academician at the Academy of Applied Radioelectronics Sciences and the recipient of the Boris Paton National Prize of Ukraine in 2021. Additionally, he serves as a Professor at the Department of Theoretical and Applied Sciences, eCampus University in Italy. His research primarily focuses on applied cryptology and coding theory, block-chain technologies, the Internet of Things (IoT), and the application of AI in cybersecurity.*



***IRYNA LYSENKO** holds a candidate of technical sciences degree. She is a vice academician of the Academy of Technical Sciences of Ukraine, Institute of Information Technologies. In addition, she is a senior lecturer at the Cyber Security and Software Department of the Central Ukrainian National Technical University. Her research is mainly focused on mathematical methods of cryptology and systems analysis.*

***DMYTRO PROKOPOVYCH-TKACHENKO** is a PhD in Technical Sciences, an Associate Professor, and the Head of the Department of Cybersecurity and Information Technologies at the University of Customs and Finance. He specializes in cybersecurity, cryptography, blockchain, IoT, and AI applications in information security.*

***YULIIA ULIANOVSKA** is a PhD in Technical Sciences, Associate Professor, and Head of the Department of Computer Science and Software Engineering at the University of Customs and Finance. She specializes in intelligent automated systems, methods for processing fuzzy and incomplete data, and artificial intelligence applications in decision support systems and information processing.*

***VALERII BUSHKOV** is a PhD student, Head of the State Cyber Protection Centre of the State Service of Special Communication and Information Protection of Ukraine (SSSCIP), and a postgraduate student of the Department of Software Engineering and Cybersecurity at the State University of Trade and Economics. He specializes in cybersecurity, information security, cryptography, and electronic communications.*