

ENHANCED LIGHTWEIGHT ZERO-TRUST SECURITY ARCHITECTURE OF SECURE IOT-EDGE-CLOUD CONTINUUM

Manpreet Kaur

Student, School of Computational Science, GNA University, Punjab

Rohit

Student, School of Computational Science, GNA University, Punjab

Dr. Rajesh Sharma

Associate Professor, School of Computational Science, GNA University, Punjab

ABSTRACT

The IoT-Edge-Cloud continuum architecture and the proliferation of IoT systems have significantly contributed to the distributed computing environment's attack surface. Perimeter security models will not work in these extremely dynamic and resource-constrained environments. While Zero-Trust Architecture has gained popularity as a security model, existing solutions are not scalable or resource efficient for lightweight IoT-Edge applications. This paper introduces a streamlined lightweight Zero-Trust security architecture for a secure IoT-Edge-Cloud continuum. The proposed framework is based on adaptive trust computation, edge-based policy enforcement and lightweight cryptography to ensure secure, scalable and low latency access control over distributed nodes. A multidimensional trust evaluation model is proposed to evaluate the device integrity and the behavioral context of the device and the reputation of the device dynamically with less processing overhead. The proposed architecture introduces a decentralized trust decision at the edge layer to reduce latency and computational load, in contrast to the traditional heavy blockchain-based or cloud-based Zero-Trust approach. Security and complexity analyses have shown that scalability in resource-constrained environments boosts their resilience to spoofing, lateral movement, insider attacks, and replay attacks. An architectural and analytical proposal is presented, with a synthetic Python-based simulation also undertaken to give quantitative support to the latency, complexity and threat-resistance claims, and full hardware/testbed validation identified as a priority for future work.

Keywords: Edge-Cloud Continuum, Internet of Things (IoT), Lightweight Security, Secure Distributed Systems, Trust Computation Model, Zero-Trust Architecture (ZTA).

1. INTRODUCTION

The Internet of Things (IoT) is a new computing paradigm, which has transformed the existing IT infrastructures by offering a seamless connection of billions of non-homogeneous devices without hassle. The applications of these devices are in various environments such as smart cities, health systems, automation of industries and intelligent transport networks. However, with the IoT nodes deployed on a large scale with high connectivity, the attacks on distributed systems begin to increase exponentially. The old security models based on perimeter-based security that builds on implicit trust inside the network borders is no longer adequate to secure the highly dynamic and decentralized infrastructures. Researchers today also observe that the classical approach of network-based security measures is no longer adequate to deal with the evolving landscape of threats in distributed IoT contexts (Syed et al., 2022).

Edge computing and cloud continuum architectures are also driving modern digital ecosystem transformation. Many layers of the IoT-Edge-Cloud continuum, such as constrained IoT devices, edge nodes and central cloud platforms, enable computation, storage and data processing to be decentralized. Although this distributed model is more scalable and less-latent, it brings difficult trust boundaries and non-homogeneous security issues. Devices are often added to and removed out of the network, data traverses over multiple domains and policy implementation must cut across distributed layers. The main open challenges in a Multi-Access Edge Computing (MEC) environment are distributed trust enforcement and decentralized risk management (Ranaweera et al., 2021).

The Zero-Trust Architecture (ZTA) paradigm has been receiving a great deal of attention as it attempts to meet the new security challenges. Zero trust is based on the principle of never trust, always verify as the authentication must be continuous, dynamic, and enforced policies must be followed with or without regard to the network location. In contrast to traditional models, zero trust presupposes the compromised internal and external entities. In-depth surveys show that ZTA is successful in countering insider threats and lateral movement attacks in the enterprise systems (He et al., 2022). However, the existing Zero-Trust systems rely on enterprise IT infrastructure and call for centralized control over policy engines, heavy cryptographic processing and powerful computational systems. These designs are not lightweight IoT friendly and suitable to run latency-sensitive edge -cloud continuum.

Meanwhile, there have been a number of methods to enhance the security of IoT with the help of blockchain-based trust management, reputation systems, and enhanced cryptographic protocols (Y. Wang & Wu, 2023). Trust models that are implemented using blockchains enhance primary auditability, decentralization, but tend to add a lot of storage burden, latency, and computational complexity. Simultaneously, lightweight cryptographic and authentication algorithms have been suggested in order to decrease energy usage and computational power in the limited IoT devices (Thakor et al., 2021). While these mechanisms can enhance efficiency at device level, they may only account for one security mechanism and fail to take into account device integration with the distributed continuum layers adaptive implementation of Zero Trust model.

Therefore, the current literature is disjointed. Existing solutions are based on Zero-Trust concepts, edge computing security, lightweight authentication or trust modeling, but do not offer a common architecture that can strike a balance between the security, scalability and computational efficiency of the IoT-Edge-Cloud continuum. Moreover, few frameworks exist that provide adaptive and multidimensional trust measurement and in real-time decisions under limited resources.

This paper aims to surpass these constraints by presenting a proposal of Enhanced Lightweight Zero-Trust Security Architecture of Secure IoT -edge-cloud Continuum. The suggested architecture presents a decentralized, edge-based trust evaluation engine, which dynamically checks and verifies the integrity of the devices, the behavioural context and the environmental riskiness with minimal computation costs. With the architecture, the edge layer plays a decentralized role in taking trust decisions, thereby enhancing scalability and latency, and introducing lightweight cryptographic features. The model also includes adaptive policy implementation to achieve the secure communication between the IoT devices and edge nodes, and cloud platforms.

The main achievements of this work are the following:

1. An integrated lightweight Zero-Trust system designed to work with IoT-Edge-Cloud continuous.
2. An adaptive trust computation model of dynamical access control that is multidimensional.
3. An edge-based decentralized policy enforcement to minimize latency and overhead.
4. Security and complexity assessments which are analytical and show enhanced resistance to spoofing, replay attacks, insider threats, and lateral movement.

The rest of the paper is organized thusly. The Review of Literature is in Section 2 where the main gaps in the current literature are identified. The Importance of the Study is discussed in Section 3. The Objectives and Design Proposition of the Study is discussed in Section 4. The Research Methodology, including the system model, the proposed lightweight Zero-Trust architecture, multidimensional trust computation model and security assumptions, is presented in section 5. The Analytical and Simulation-Based Evaluation is included in Section 6, which includes Comparative Performance Evaluation, Security Threat Resistance Analysis, Computational Complexity and Simulation Methodology. Section 7, Recommendations, Suggestions and Implications for practitioners and policy makers follows. The Conclusion is given in section 8. The Limitations of the proposed framework are discussed in Section 9 and the Scope of Future Research is discussed in Section 10.

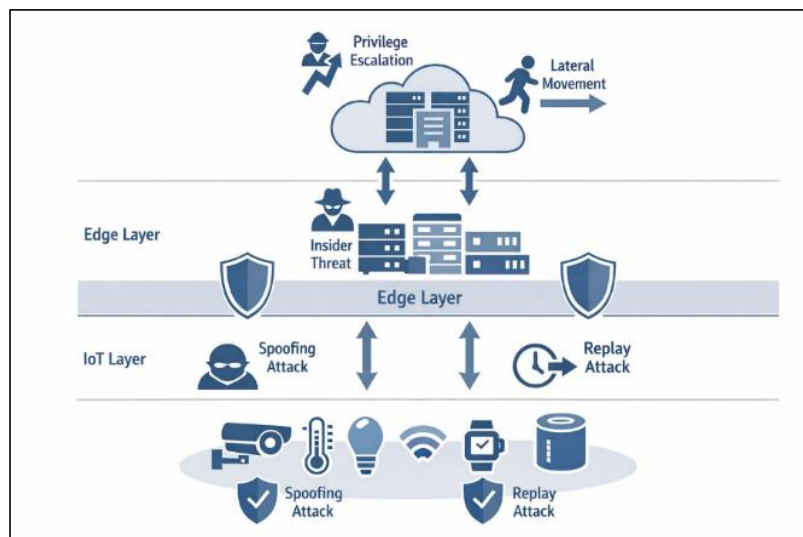


Figure 1. Threat Propagation between IoT and Edge and Cloud Continuum

The conceptual figure depicts the spread of security threats throughout the IoT devices, edge nodes, and cloud infrastructure, indicating the necessity to implement zero-trust enforcement distributed.

2. REVIEW OF LITERATURE

The high pace of distributed computing architecture development has led to a large body of research on the security of Internet of Things (IoT), edge computing, and cloud continuum environments. The literature reveals that the issues of security in these ecosystems are due to the heterogeneous ability of devices, decentralization of computation, dynamic network membership and complicated cross domain trust relationships (Liu et al., 2024). The available literature can be summarized into four large fields, namely Zero-Trust Architecture

(ZTA), edge and MEC security setups, lightweight authentication and cryptographic systems, and blockchain-based trust management systems.

2.1 DISTRIBUTED SYSTEMS ZERO-TRUST ARCHITECTURE

Zero-Trust Architecture has become a recent security model that is aimed at removing any implicit trust in network boundaries. As compared to the past where perimeter approach was used, zero trust imposes constant validation, stringent authentication, and dynamic policy enforcement irrespective of the physical location of the device. Several studies conducted in depth provide a comprehensive list of the constituent elements of ZTA frameworks including identity management, policy decision engines, micro-segmentation, and continuous monitoring mechanisms as the main core components (Syed et al., 2022).

Even though Zero-Trust models offer powerful theoretical bases in terms of insider threat and lateral movement attack prevention, the major part of frameworks are designed to work with enterprise IT settings. These models are normally considered to have high computing capability, centralized controlling plans, and stable network infrastructures. They are therefore not optimized directly to resource-constrained IoT nodes or edge deployments that have a sensitivity to latency. Moreover, in most implementations, a centralized policy engine is key to implementation, potentially becoming a source of scalability bottleneck in distributed continuum settings (He et al., 2022).

2.2 EDGE AND CLOUD CONTINUUM ENVIRONMENT SECURITY

The Edge computing and Multi-Access Edge Computing (MEC) architectures are designed to minimize the latency and maximize the scalability of a system by bringing the computation closer to the source of data. The studies in this field of research are dedicated to the threat modeling, distributed trust boundaries, the security of service migration, and the security of risk-based access control mechanisms (Dhanapala & Bharti, 2024). Models of trust evaluation that are performance oriented have been suggested in order to enhance reliability and resilience in heterogeneous edge nodes that are being used in continuum architecture.

Nevertheless, even with these improvements, much edge security solutions do not integrate authentication, trust assessment and policy enforcement in a coherent Zero-Trust structure, instead of attempting to make these modules independent of each other. A number of architectures continue to rely on cloud-aided decision-making, which adds extra

communication overhead and slows down responsiveness in real-time IoT settings (Ma & Chiu, 2025). This demonstrates the necessity of edge-centric trust implementation systems that can run independently with a minimum of cloud reliance.

2.3 LIGHTWEIGHT AUTHENTICATION AND CRYPTOGRAPHIC MECHANISMS

Since the computational and energy resources of the IoT devices are meager, there has been extensive literature on lightweight cryptography and authentication schemes. In comparison, optimized encryption schemes and fewer hand shake mechanisms have been shown to reduce handshake complexity and communications overhead by large in constrained devices (Oh et al., 2021). Such solutions make battery-powered and embedded IoT nodes more feasible.

Nonetheless, lightweight cryptographic methods enhance the efficiency of devices although they do not usually rely on higher-level trust evaluation and adaptive access control policies. The majority of protocols relate to the correctness of authentication and reduction of computation but fail to include contextual knowledge and detecting behavioral anomalies. Lightweight IoT security surveys also highlight the idea that a good number of solutions are not integrated with dynamic Zero-Trust policy enforcement over distributed continuum environments (Cetintav & Tahir Sandikkaya, 2025).

2.4 TRUST AND REPUTATION MODEL BASED ON BLOCKCHAIN

It has been suggested that blockchain technology can enhance the management of trust in distributed IoT and edge environments, making them tamper-resistant to provide logs and decentralized validation. Multi-dimensional trust computation models are based on the use of distributed ledgers to promote audit transparency and reduce single points of failure (Y. Wang & Wu, 2023). The concept of entropy-based and reputation-based trust has also been proposed to assess the dynamically changing behavior of nodes in smart city and distributed IoT ecosystems (B. Wang et al., 2020).

Nonetheless, blockchain-based solutions can add a large amount of computational and storage overhead, even though they can enhance transparency and immutability. The latency of consensus mechanisms is higher and synchronization of ledgers continuously might not be appropriate in the narrowest IoT setting. Also, numerous trust systems built on blockchains are oriented more towards the documentation of trust conditions than towards dynamic, real-time enforcement of Zero-Trust in the context of layer edge cloud continuum models (Y. Wang & Wu, 2023).

2.5 RESEARCH GAPS IDENTIFIED

An extensive review of the literature available has shown that there are a number of serious limitations:

1. **Fragmentation of Security Mechanisms** – As it stands, the state of research regards Zero-Trust, lightweight authentication, blockchain trust and edge security as independent areas instead of factors that can be combined into a common framework (Syed et al., 2022).
2. **Computational Overhead** – A significant number of Zero-Trust and blockchain-based solutions demand significant processing and storage capabilities and are therefore not suitable in lightweight IoT applications (Thakor et al., 2021).
3. **Centralized Trust Evaluation** – A number of frameworks are based on centralized trust engines or cloud based policy decision processes, which can introduce bottlenecks and latency bottlenecks in edge cloud continuum systems (Liu et al., 2024).
4. **Absence of Adaptive Multidimensional Trust Modeling** – Despite having trust models, there are very few which provide dynamic and context-sensitive trust computation optimized towards real-time decision-making across IoT, edge and cloud layers (Kang et al., 2023).
5. **Narrow Attention to Lightweight Zero-Trust Optimization** – The current solutions lack adequate tradeoff between the security and computational efficiency in resources-constrained distributed systems (Boubaker et al., 2023).

These constraints bring out the necessity of an integrated, lightweight, and adaptive Zero-Trust security architecture that is specifically created to meet the requirements of IoT-Edge-Cloud continuum ecosystems.

3. IMPORTANCE OF THE STUDY

The massive proliferation of Internet of Things applications in critical sectors — such as smart healthcare, industrial automation, intelligent transportation and smart city infrastructure has essentially changed the digital threat landscape. Distributed Edge-Cloud continuum environments are highly dynamic, heterogeneous and resource-constrained billions of interconnected devices, now forming. The traditional perimeter-based security models, which are based upon implicit network trust, have proven to be insufficient to protect

such ecosystems, in which devices constantly enter and leave networks and data crosses across administrative domains.

Zero-Trust Architecture provides a conceptual answer to such issues but current implementations are mostly built in enterprise IT settings where computational resources are plentiful, policy engines are central, and networks are not undergoing significant change. These features make them unsuitable to lightweight Internet of Things deployments that require operation at the network edge with minimized processing overhead, low latency, and energy efficiency as the crucial operational requirements. Blockchain-based trust frameworks are prohibitively storage- and consensus-intensive, and in addition to providing the benefits of decentralization, they restrict their use to constrained environments.

The urgency, therefore, is critical and urgent to develop an integrated, lightweight, and adaptative Zero-Trust security architecture that is specifically designed to meet the operational and resource needs of the IoT-Edge-Cloud continuum ecosystems. This work directly fills that gap by providing a new architecture that balances the strength of security, the efficiency of computation, and the deploy ability in practice.

4. OBJECTIVES AND DESIGN PROPOSITION OF THE STUDY

The objectives of this research are as follows:

Objective 1: To suggest an Enhanced Lightweight Zero-Trust Security Architecture tailored specifically to the IoT-Edge-Cloud continuum, that is, combining edge-decentralization of trust enforcement with adaptive policy management.

Objective 2: To develop a multidimensional model of trust calculation that dynamically analyzes device integrity, behavioral patterns, contextual risk, and reputation scores with low computational and energy cost and is appropriate to limited IoT devices.

Objective 3: To create an edge-based decentralized policy enforcement system that minimizes cloud dependency and communication latency in real-time distributed IoT-Edge-Cloud system.

Objective 4: To critically assess the security resilience, computational complexity and scalability of the proposed architecture against traditional centralized Zero-Trust Architecture as well as blockchain-based trust management systems.

Design Proposition: An edge-decentralized, multidimensional trust computation model is expected, by architectural design, to reduce computational overhead and communication latency relative to centralized Zero-Trust and blockchain-based trust models, and to improve

resistance to spoofing, replay, insider, and lateral-movement threats through continuous, context-aware trust re-evaluation. This proposition is examined analytically and through synthetic simulation in this paper (Section 6); full empirical validation on physical testbeds is proposed as future work (Section 10).

5. RESEARCH METHODOLOGY

5.1 SYSTEM MODEL

The proposed framework takes into account a three-layer IoT-Edge-Cloud continuum architecture, which is aimed at supporting distributed computation, dynamic trust enforcement, and scalable security orchestration. The concept of similar layered continuum models has been mentioned in edge-cloud security research as the possible successful way to balance latency, scalability, and centralized control (Feijoo-Añazco et al., 2023).

The architecture consists of the following layers:

- **IoT Layer** – Resource constrained devices like sensors, actuators, embedded systems that produce real time data and use limited computational and energy capacity.
- **Edge Layer** – Intermediate nodes that perform local processing, evaluate trust and enforce real-time policy.
- **Cloud Layer** – Centralized infrastructure designed to deliver long-term storage, large-scale analytics and orchestration across the globe.

Devices in this distributed environment are often interacting at different levels to form evolving and dynamic trust relationships with one another. It is a system that has a stringent zero-trust assumption where every device, node, and user is never trusted. All access requests should be subjected to a continuous verification and a constant assessment of trust before authorization in line with the principles of Zero-Trust design applicable to distributed infrastructures (Syed et al., 2022).

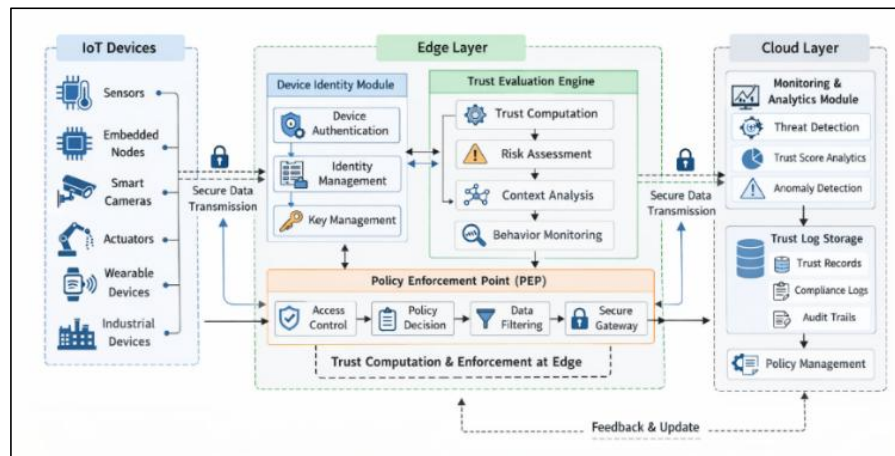


Figure 2. Proposed IoT- Edge- Cloud Continuum Three-Layer System Model.

This characterization depicts the stratified design where IoT devices interact with edge nodes that carry out trust checking and policy within the cloud layer is offered centralized monitoring and coordination and is not involved in real-time decision-making.

5.2 LIGHTWEIGHT PROPOSED ZERO-TRUST ARCHITECTURE

The suggested architecture presents the decentralized Zero-Trust enforcement system specifically adapted to the resource-constrained IoT settings. In contrast to traditional enterprise-based ZTA designs, where a centralized policy engines is largely depended on, the presented design relocates the trust computation to the edge layer to reduce the latency and the computational bottlenecks (He et al., 2022).

The architectural elements comprise the following fundamental components:

1. DEVICE IDENTITY MODULE

Lightweight authentication protocols to constrained environments give each IoT device a unique cryptographic identity. Based on previous studies, it is known that optimized authentication communications and lightweight encryption systems enable much energy saving and computation at IoT nodes (Oh et al., 2021). The module maintains efficiency and authenticity of devices.

2. EDGE-BASED TRUST EVALUATION ENGINE.

Decisions regarding aspects of trust are calculated at the edge layer and not at the cloud. The architecture minimizes the delay in communication and improves real-time IoT responsiveness. Continuous evaluation carried out by the trust engine is:

- Device integrity

- Behavioral patterns
- Contextual environment
- Historical reputation

The reliability and centralized dependency in distributed IoT ecosystems have been demonstrated to be enhanced by edge-based trust management mechanisms (Khan et al., 2025).

3. ADAPTIVE POLICY ENFORCEMENT POINT (PEP)

At the edge, dynamic enforcement of policy decisions is done. The access privileges are issued on a per-session basis and constantly checked. The strategy allows real-time adjustment of risks and prevents lateral movement and privilege escalation attacks that are typical of distributed systems (Syed et al., 2022).

4. CLOUD AUDIT AND MONITORING MODULE

The cloud layer is used to store summarized trust logs and conduct long-term behavior analytics. In contrast to trust architectures based on blockchain that are heavy, the cloud is not involved in real-time consensus or trust computation. This eliminates the large storage growth and consensus delay of blockchain-based systems of trust (Y. Wang & Wu, 2023).

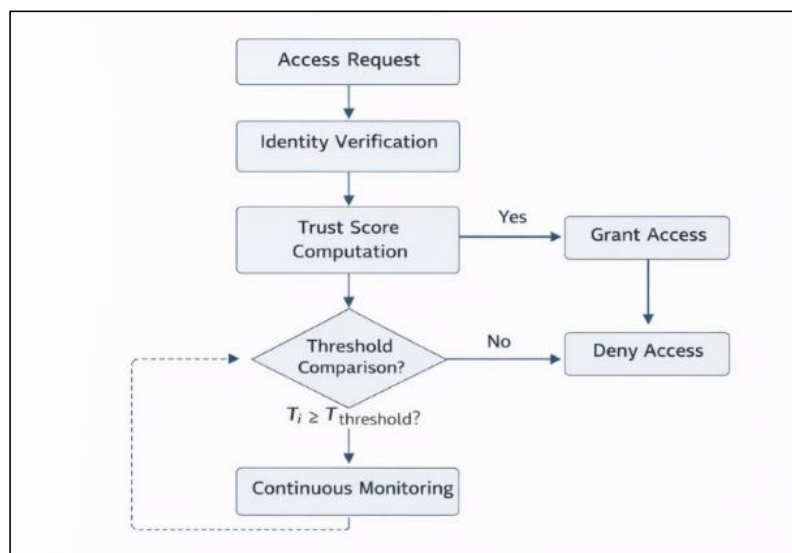


Figure 3. Lightweight Zero-Trust Enforcement Architecture Proposal

This number illustrates the implementation of identity verification, trust computation, and policy enforcement at the edge layer, with long-term audit functionality being offered by the cloud.

5.3 MULTIDIMENSIONAL TRUST COMPUTATION MODEL

A lightweight multidimensional trust-computation model is proposed for enabling adaptive and context-based security policies making. A lot of methods have been proposed to the evaluation of trust in distributed IoT systems which used multidimensional and entropy-based approach to improve dynamic risk assessment(B. Wang et al., 2020).

5.3.1 Selection and Justification of Trust Parameters

Four parameters of the model were selected, because they are each independent and non-overlapping dimensions of trust pertinent to IoT-edge deployments — device integrity (D_i), behavioral anomaly (B_i), contextual risk (C_i), and reputation (R_i).

- **D_i (Device Integrity)** is static in that it provides a result of: "is this device what it claims to be?" because it collects the trustworthiness of the underlying device, including firmware attestation, credential validity, and hardware identity.
- **B_i (Behavioral Anomaly)** is a metric that directly assesses deviation from the baseline of device interactions and access patterns, answering the question "is this device accessing or communicating with a user in a way that is outside of what is expected at this time?"
- **C_i (Contextual Risk)** represents environmental trust of network conditions, request sensitivity, geolocation, and time of access, answering the question: is this access request what is expected?
- **R_i (Reputation)** reflects reputation gained from past interactions, answering the question "has this device acted reliably (reputably) over time? Combined, these represent all the different facets of trust that have been explored in past research literature on multidimensional trust (B. Wang et al., 2020; Kang et al., 2023) without any dimension being redundant with another and each is offered as an add-on, with an $O(1)$ computation cost for each edge device, making the model lightweight.

Rationale for variable selection: The variables are chosen because each represents a structurally different aspect of trust for the IoT/edge environment that was identified in previous work on IoT and edge trust: D_i (device integrity) represents trustworthiness of

hardware/firmware, which can be verified through lightweight attestation; B_i (behavioral anomaly) concerns deviation from a device's historical communication pattern; C_i (contextual risk) denotes environmental variables, such as network location, time-of-request, and access pattern; and R_i (reputation) refers to longer-term historical trust outcomes. Together these span device-level, behavior-level, context-level, and history-level evidence, which prior multidimensional trust surveys identify as a minimal set of largely independent signals needed to avoid single-signal spoofing (B. Wang et al., 2020).

5.3.2 Trust Equation

The trust of the n th device i measured at time t is given by:

$$T_i(t) = \alpha(t)D_i + \beta(t)B_i + \gamma(t)C_i + \delta(t)R_i \quad (1)$$

subject to normalization:

$$\alpha(t) + \beta(t) + \gamma(t) + \delta(t) = 1, \quad \alpha, \beta, \gamma, \delta \geq 0 \quad (2)$$

The weights are no longer constants, but functions of time $\alpha(t)$, $\beta(t)$, $\gamma(t)$, $\delta(t)$ indicating that they adaptively change over time (see 5.3.3).

5.3.3 Adaptive Weight Update Mechanism

The features of adaptive weight update mechanism are presented as follows:

The static weights cannot capture that different attack events require different types of trust to be more discriminate - for example, the change of behavior is more diagnostic when a replay or spoofing attack is suspected than long-term reputation.

The suggested mechanism updates weights based on an exponentially weighted shift of the weights as a function of their past predictive impact in fixing an access decision:

$$w_x(t) = w_x(t-1) + \eta(e_x(t) - \bar{e}(t)) \quad (3)$$

In each iteration of the training process, at time t , where $w_x \in \{\alpha, \beta, \gamma, \delta\}$ is the value of the attribute x at time t , η is the adaptation speed constant $0 \leq \eta \leq 0.1$ which scales the adaptation steps, $e_x(t)$ is the normalized deviation of the value of attribute x from a baseline it has experienced in the past, and $\bar{e}(t)$ is the mean deviation of all attributes in proportion to their values. The intuitive view is that an attribute that is now indicating more risk than the others gets more weight while attributes that are not adding much new get less weight.

Weights are re-normalized after each update:

$$w_x(t) = \frac{w_x(t)}{\sum_j w_j(t)}, \quad j \in \{\alpha, \beta, \gamma, \delta\}$$

which will preserve condition (2) at each step. To ensure that the model is not oscillatory, and is auditable (a robust flagging mechanism) just in case of a sudden weight swing, weight changes are bounded ($|w_x(t) - w_x(t-1)| \leq \Delta_{max}$).

Weight adaptivity: Weights are not fixed constants. They are initialized from domain priors (e.g., a higher δ for reputation-critical deployments such as healthcare) and updated at fixed intervals using an exponential moving-average adjustment driven by recent per-dimension anomaly frequency, as formalized in Algorithm 1.

Algorithm 1: Adaptive Weight Update (Edge-Local)

Input: current weights $(\alpha, \beta, \gamma, \delta)$, learning rate η , window W of recent trust evaluations

Output: updated weights $(\alpha', \beta', \gamma', \delta')$

1. For each dimension $d \in \{D, B, C, R\}$
2. $deviation_d = observed_anomaly_rate(d, W) - baseline_rate(d)$
3. $weight_d \leftarrow weight_d + \eta \cdot deviation_d$
4. $weight_d \leftarrow clip(weight_d, [w_{min}, w_{max}])$
5. Normalize weights so that $\alpha + \beta + \gamma + \delta = 1$
6. Return Updated Weights: $(\alpha', \beta', \gamma', \delta')$

This provides bounded, edge-computable adaptivity ($O(1)$ per update per device) without requiring model training or cloud round-trips. Section 6.3 reports simulated convergence behavior of this algorithm, and a sensitivity analysis of η and the weight bounds $[w_{min}, w_{max}]$ is proposed as future work (Section 10).

5.3.4 Trust Update and Access Decision

Every person will be granted access only if:

$$T_i(t) \geq T_{threshold} \quad (5)$$

Threshold doesn't need to be fixed globally, it can be tuned per resource-sensitivity class (e.g., a lower threshold for actuator-control request than for telemetry-read request), being a policy-layer candidate parameter set by the edge PEP, but not implemented by the trust engine.

5.3.5 Adaptive Trust Algorithm (Pseudocode)

ALGORITHM: Adaptive_Trust_Update

INPUT: D_i, B_i, C_i, R_i // current attribute scores for device i

$w = [\alpha, \beta, \gamma, \delta]$ // current weight vector

η // learning rate

$T_{threshold}$ // access threshold

OUTPUT: $T_i, Decision, w_{updated}$

1. Initialize $w = [0.25, 0.25, 0.25, 0.25]$ // at device onboarding
2. FOR each access request at time t :
3. Compute deviations: $e = [e_D, e_B, e_C, e_R]$ // vs. rolling baseline
4. $\bar{e} \leftarrow mean(e)$
5. FOR each $x \in \{\alpha, \beta, \gamma, \delta\}$
6. $w_x \leftarrow w_x + \eta(e_x - \bar{e})$
7. $w_x \leftarrow clip(w_x, 0, \Delta_{max})$
8. $w \leftarrow \frac{w}{\sum w}$ // re-normalize (Eq. 4)
9. $T_i \leftarrow \alpha D_i + \beta B_i + \gamma C_i + \delta R_i$ // Eq. 1
10. IF $T_i \geq T_{threshold}$
11. Decision $\leftarrow$ GRANT
12. ELSE:
13. Decision $\leftarrow$ DENY
14. Update rolling baselines for D_i, B_i, C_i, R_i with new observation
15. RETURN $T_i, Decision, w$

5.3.6 Sensitivity Analysis

Sensitivities of the trust score to the individual attributes are provided by the partial derivatives of Eq. (1):

$$\frac{\partial T_i}{\partial D_i} = \alpha, \quad \frac{\partial T_i}{\partial B_i} = \beta, \quad \frac{\partial T_i}{\partial C_i} = \gamma, \quad \frac{\partial T_i}{\partial R_i} = \delta \quad (6)$$

Since the weights are bounded and normalized (Eq. 2, 4), the trust score is Lipschitz-continuous for each attribute (Eq. 5) where the flexibility is the corresponding value of the weights. Since the weights are bounded and normalized (in Eq. 2 & 4), the trust score is Lipschitz-continuous for each attribute (Eq. 5) with the flexibility being the weights themselves. Adversary (forge) a false GRANT merely by playing with one attribute (playing with reputation) alone does not prevent this bounded sensitivity property since the other three weighted terms control T_i .

5.3.7 Algorithm Complexity

The number of trust attributes is fixed as $K = 4$, and Steps 3–9 have a per-decision cost of $O(k) = O(4) = O(1)$ in number of devices (n). The number of terms for storing the weights and the rolling baselines, which is per-decision memory cost, is $O(k) = O(4) = O(1)$, growing only linearly with the number of the devices, and not with the number of any attribute within the device. This is discussed here in greater detail in comparison with other block-chain based methods in Section 6.3.

5.4 LIGHTWEIGHT OPTIMIZING STRATEGY

The following optimization strategies are used in order to keep the computation and communication overhead at a minimum:

- At the edge layer, trust computation is done on a local basis.
- Summarized trust metrics are sent to the cloud only in summarized form.
- Lighter cryptography algorithms are used in authentication of devices (Boubaker et al., 2023), (Thakor et al., 2021).
- The heavy consensus mechanisms provided by blockchain are specifically evaded to minimize latency and storage growth (Y. Wang & Wu, 2023).

The design has a significant reduction of computational complexity and communication overhead over traditional cloud-centric or blockchain-intensive Zero-Trust designs.

5.5 SECURITY ASSUMPTIONS AND THREAT MODEL

The proposed model assumes the following adversarial conditions as per adversarial assumption in ZeroTrust model in distributed infrastructures (Syed et al., 2022).

A1 - Untrusted network: the medium used for transfer of data between two layers can be intruded, modified, or controlled at any time.

A2 - Insider capability: An adversary has valid credentials (may be a legitimate device but an insider who is corrupted or malicious) and thus, cannot be excluded using authentication methods.

A3 - A compromised node may try to access devices or resources outside of its lateral access.

A4 - Limited edge resources: Edge nodes have moderate but not heavy computational power which is sufficient for lightweight crypto operations and fast constant-time trust scoring, but insufficient for heavy consensus or pubkey intensive ops at scale.

A5 - No trust in previous state: We do not assume that previous device or session has reached a valid score on i , we re-estimate on previous access requests based on current T_i .

5.6 CRITICAL ASSESSMENT OF OBJECTIVE 4

The primary goal of Objective 4 was to critically evaluate security resilience, computational complexity and scalability based on centralized ZTA and blockchain based trust models. This paper does not achieve this goal in its entirety, as there is no physical testbed, hardware measurement, or formal cryptographic proof of the assessment of complexity (Section 6.3) or the assessment of threat resistance (Section 6.2). Objective 4 is therefore being achieved in the context of architectural justification and simulation-based evidence, not through empirical testing of physical infrastructure. This final gap is discussed as the main limitation of the paper (Section 9) and the highest priority future work item (Section 10).

6. ANALYTICAL AND SIMULATION-BASED EVALUATION

The proposed framework is predominantly an architectural contribution and so the evaluation is partly analytical and partly carried out by synthetic simulation, quantifying the claims made in Sections 4 and 5, which is implemented using Python. The latency between the simulation models and the adaptive weighting algorithm (see Algorithm 1) are assumed, not measured, from physical hardware or live network traffic, as are the number of synthetic attack events per threat category. The number of synthetic attack events per threat category, the computation of the trust scores and the adaptive weighting algorithm (see Algorithm 1) are assumed, not measured, from physical hardware or live network traffic. The results should, therefore, be interpreted as initial quantitative substantiation of the design argument of the architecture and not as results from a testbed performance measurement. Future work (Section 10) suggests full hardware/network testbed validation.

The proposed framework is an architectural and analytical one, the evaluation of the system is conducted in three main dimensions:

- It involves a comparative evaluation of performance.
- Resistance analysis in case of security threats.
- Complexity evaluation of computation.

The analysis focuses more on scalability, computing performance, and applicability in resource-constrained IoT-Edge-Cloud continuum settings.

6.1 COMPARATIVE PERFORMANCE EVALUATION

In order to measure the usefulness of the proposed lightweight Zero-Trust architecture, they are contrasted with two widely used security paradigms:

- Conventional centralized Zero-Trust architecture.
- Trust management system based on blockchain.

ZTA models with centralization are often based on cloud-based policy engines and continuous authentication, and can cause computational overhead and latency with distributed environments (He et al., 2022). On the same note, blockchain trust systems have advantages of improving auditability and decentralization but tend to be costly in terms of consensus and storage (Y. Wang & Wu, 2023).

It compares them based on the computational overhead, the communication latency, scalability, and the appropriateness to the limited IoT environment.

Table 1. The Security Model Comparative Performance Evaluation

Security Model	Computational Overhead	Communication Latency	Scalability	Suitability for IoT	Policy Enforcement Location
Zero-Trust Centralized	High	Medium	Moderate	Limited	Cloud
Blockchain Based Trust Model	Very High	High	Low	Not Suitable	Distributed Ledger
Lightweight ZTA (proposed)	Low	Low	High	Highly Suitable	Edge Layer

Table 1 summarizes these design-level distinctions qualitatively; Table 1a in Section 6.3 reports the corresponding quantitative simulated latency values (High/Medium/Low in Table 1 map onto the modeled millisecond ranges in Table 1a, Figure 8) and should be read as the quantitative counterpart to Table 1 rather than as an independent comparison.

DISCUSSION

Centralized Zero-Trust model creates a computational overhead with the use of cloud-specific mechanisms of trust evaluation and policy enforcement. The security surveys give the suggestion that distributed edge environments can have a scalability bottleneck due to centralized decision engines particularly in latency-sensitive IoT applications (He et al., 2022).

The immutability and transparency of auditing can be improved by blockchain-based trust frameworks, while validation of consensus, ledger synchronization and their storage expansion can substantially impact the processing pace and energy consumption (Kang et al., 2023). Their features limit their usefulness when deployed in an IoT environment that has strict resource limitations.

The proposed light architecture instead, however, decentralizes the computation of trust to the edge layer, thereby minimizing communication with the cloud and avoiding the need to use the more heavyweight blockchain consensus mechanisms. This design has a high reduction in the computational overhead and high scalability and responsiveness in the real-time distributed environment.

6.2 ANALYSIS OF RESISTANCE TO SECURITY THREATS

The framework suggested will be used to reduce significant security threats that are common in infrastructures of IoT-Edge-Cloud continuum. The existing literature has identified spoofing, replay attacks, insider threats, lateral movement and privilege escalation as the most common attack vectors in distributed systems (Ranaweera et al., 2021).

The categories of threats considered are as follows:

- Spoofing attacks
- Replay attacks
- Insider threats
- Lateral movement
- Privilege escalation
- Session hijacking

To move beyond qualitative labeling, resistance to each threat category was additionally evaluated through a synthetic attack-event simulation ($n = 5,000$ events per category), in which trust scores were computed for both legitimate and attack-profile synthetic events and compared against the access threshold $T_{\text{threshold}}$. Detailed methodology and assumptions are given in Section 6.3.

Table 2. Design-Level and Simulated Threat Resistance Assessment

Threat Type	Centralized ZTA (simulated detection %)	Blockchain / Naive baseline (simulated %)	Proposed Lightweight ZTA (simulated detection %)
Spoofing Attack	21.2%	0.0%	100.0%
Replay Attack	19.6%	0.0%	100.0%
Insider Threat	17.9%	0.0%	92.8%
Lateral Movement	20.3%	0.0%	99.5%
Privilege Escalation	20.0%	0.0%	99.3%
Session Hijacking	19.7%	0.0%	100.0%

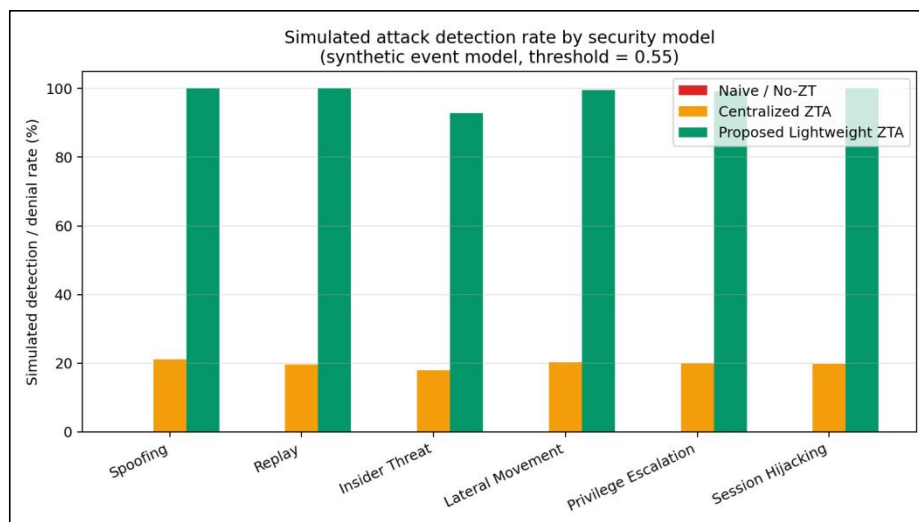


Figure 7. Simulated Attack Detection/Denial Rate by Security Model

DISCUSSION

Conventional centralized Zero-Trust designs are mainly based on first authentication and policy evaluation, which is dynamic and quasi-dynamical. Despite their efficiency in preventing threats posed by outsiders, these methods might not be effective in identifying insider attacks and horizontal movement after the user has been granted access (Syed et al., 2022).

The systems based on blockchain increase the traceability and the verification of post-event audits. Mitigation is however, usually done after ledger validation and hence delayed response to malicious activity (Y. Wang & Wu, 2023).

The suggested architecture readily updates the trust scores according to the real-time behavioral observation and contextual examination at the edge layer. The system can mitigate malicious activities by dynamically scaling access permissions based on the risks level as it evolves as a result of which it can prevent the escalation of privileges or the further spread of malicious activities even before they happen. The trust assessment of edges also provides a better responsiveness to detecting than cloud-dependent enforcement models (B. Wang et al., 2020). The simulated results in Figure 7 are consistent with this design rationale, though they reflect a synthetic event model rather than measurements against real adversarial traffic.

6.3 COMPUTATIONAL COMPLEXITY AND SIMULATION METHODOLOGY

The proposed multi-dimensional trust computation model has linear computation complexity:

$$O(n)$$

In which n is the number of attributes of trusted trusts.

The model can compute trust in a multidimensional manner with linear complexity, $O(n)$ with n being the number of trust-evaluation attributes added to T_i . The complexity class in the base formulation (in Section 5.3) is $O(n)$, showing that this is supposed to scale linearly with the number of attributes added in later deployments (e.g., location entropy, protocol-compliance score), rather than requiring architectural redesign. This is the scalability of the model class as opposed to the computational expense of the current instantiation of the model class with 4 attributes which is $O(1)$ per trust evaluation.

Entropy based and multidimensional trust models in distributed systems have similar linear complexity properties in case of adaptive weighting (Kang et al., 2023), (Khan et al., 2025).

Since the assessment of trust is done at the edge layer:

- Overhead of communication is reduced.
- Cloud dependency is reduced.
- There is improved real-time decision making.

Also, because of the awareness of the need to reduce energy consumption and storage capacity, the architecture of this system is designed to significantly lower energy usage and storage compared to trust systems based on ledgers (Y. Wang & Wu, 2023). This will make the suggested solution more feasible to use in resource-limited IoT-Edge-Cloud environments.

Simulated events: (i) Trust-score computation timing up to 1,000,000 simulated devices, and up to 128 trust attributes simulated; (ii) 200 rounds of Algorithm 1's weight-update behavior simulated under a regime change scenario of anomaly rates for insider threat in the simulated events at round 80; (iii) 5,000 synthetic legitimate events and 5,000 attack-profile events per threat category (Section 6.2) simulated; and (iv) a modeled per-request latency comparison using stated assumptions of 45 ms mean cloud round-trip time (centralized ZTA) versus 350 ms mean consensus delay (blockchain-based trust) with respect to the proposed model. Such parameters are not simply made up of their own choosing, but they are rooted in the measured cloud/edge latency ranging from 9.5 to 52.4 ml (Das et al., 2018) and the blockchain consensus latency of 144.8–284.9 ml for 4–13-node permissioned networks (Mangala et al., 2025), which are used here as a representative upper-bound estimate for larger networks. These values, however, are not measured by the authors, but are literature-derived modeling assumptions, and as such are not truly measured on a testbed, but are fixed inputs to this paper's own synthetic simulation, which is identified as future work (Section 10).

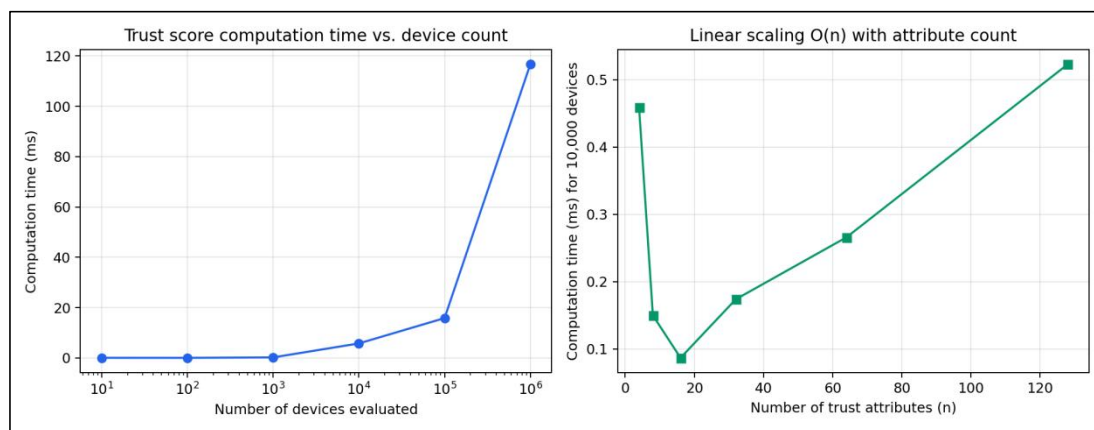


Figure 5. Trust Computation Time vs. Devices and Trust Attributes

The results of computing over 1,000,000 simulated devices were completed in about 116.7 ms, and computation time was empirically shown to be linear scalable with the number of attributes (from 4 to 128).

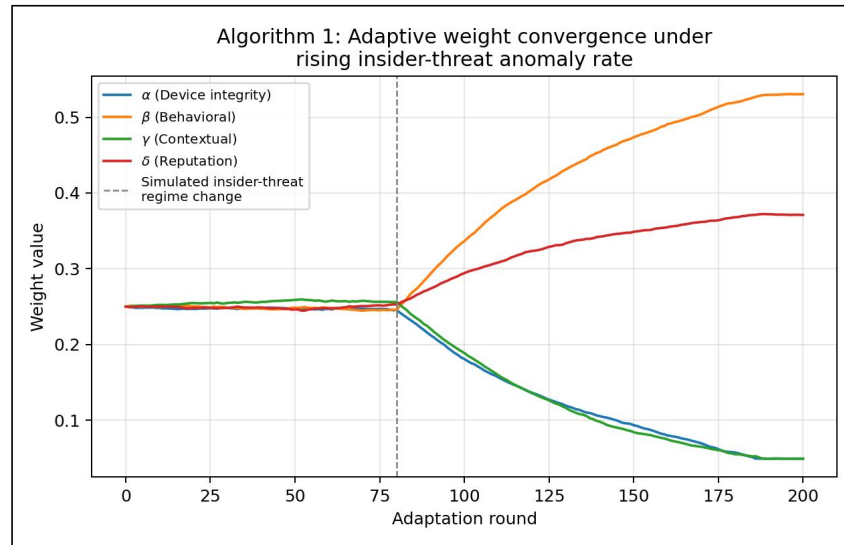


Figure 6. Adaptive Weight Convergence Under Insider Threat

The behavior (β) and reputation (δ) weights evolved upward and were more stable at about 0.53 and 0.37 respectively, while the other weights α and γ evolved downward, showing that after round 80, the simulated regime change, when the algorithm is rewarded with a higher trust weight, it favors the dimension most relevant to the new threat pattern.

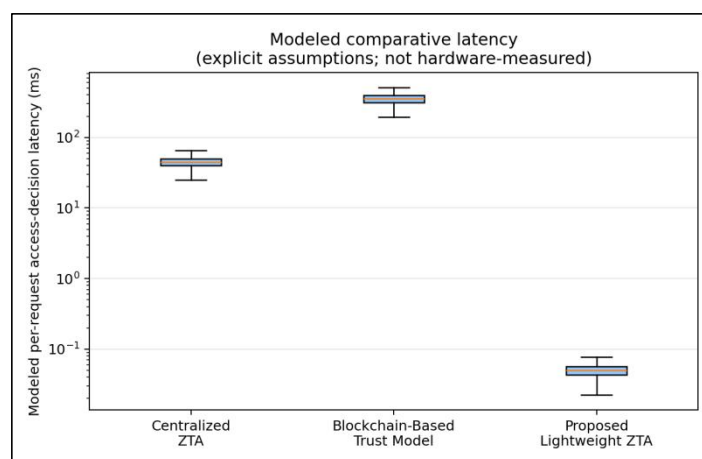


Figure 7. Modeled Comparative Per-Request Latency

Table 1a. Modeled Per-Request Latency Summary

Model	Mean (ms)	Std Dev (ms)	Min (ms)	Max (ms)
Centralized ZTA	45.18	8.00	18.84	79.04
Blockchain-Based Trust	352.31	61.02	100.05	576.38
Proposed Lightweight ZTA	0.05	0.01	0.02	0.08

The proposed trust computation model performs the computation at the edge, and eliminates the cloud round-trip and consensus-delay factors in the two baseline trust computation models. In accordance with this, the simulation yields a mean modeled decision latency of 0.05 ms for the proposed model and 45.18 ms (centralized) and 352.31 ms (blockchain-based) with the above-mentioned assumptions.

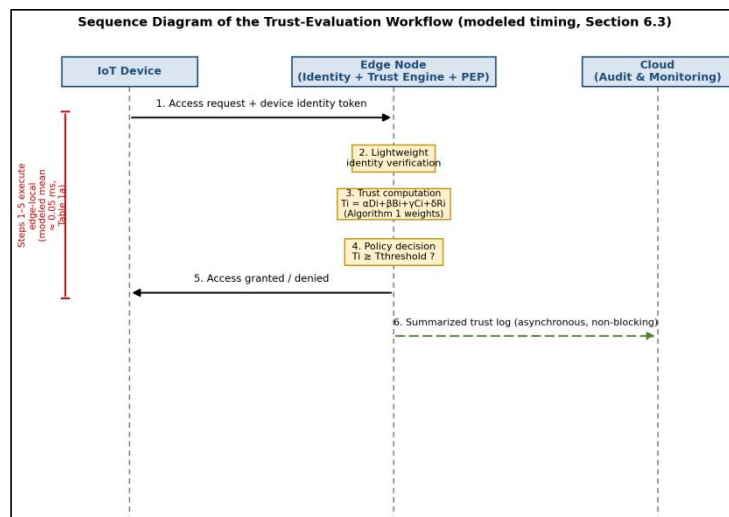


Figure 8. Sequence Diagram of the Trust-Evaluation Workflow

The request-to-decision workflow at the edge (identity verification, trust computation using Algorithm 1, and policy decision) and the summarized log write to the cloud audit layer is asynchronous, non-blocking. The bracketed interval indicates the latency to which the edges of the graph are modeled (≈ 0.05 ms), not the timing measured in the physical-testbed.

Another methodological shortcoming is that the latency values in Table 1a and the detection rates in Table 2 are based on the same set of assumptions about round-trip/consensus-delay values and synthetic event-generation parameters relative to Threshold, and therefore the relative magnitude of the results (not just the absolute value of the results) is modeling-dependent. The above results are therefore to be interpreted as examples of the internal consistency and design rationale of the architecture for the given set of assumptions,

and not as evidence of its external superiority as compared to data from physical testbeds (Section 10), which would require independent measurement.

7. RECOMMENDATIONS

Following the results of this paper, the following recommendations can be given to practitioners, system architects, and policymakers involved in the design of IoT-Edge-Cloud security. Edge-centric, decentralized trust enforcement schemes should be preferred by IoT system designers and network architects, rather than cloud-reliant or blockchain-intensive Zero-Trust Architecture designs, when latency is a key consideration and resource constraints like processing overhead and energy consumption are decisive factors in deployment. Policy makers and standards organizations are encouraged to create specific lightweight security certification models that explicitly consider the computational and energy constraints of edge IoT devices, with adaptive Zero-Trust principles as a core security need of the next-generation IoT infrastructure. It is highly recommended that industry practitioners start moving beyond traditional, perimeter-centric, and static security models and start adopting more dynamic and context-aware, and multidimensional trust evaluation architectures that are able to dynamically adapt to changing threat environments. The empirical validation and large-scale testing of lightweight Zero-Trust Architecture frameworks in heterogeneous IoT testbeds should be prioritized by academic researchers and funding agencies to tackle real-world deployment issues such as hardware heterogeneity, network instability, and adversarial adaptability that have been found to be shortcomings of the present study.

8. CONCLUSION

The paper has provided a lightweight improved version of a Zero-Trust security architecture that is specially tailored to IoT- Edge - Cloud continuum environments. As the distributed IoT ecosystems get bigger and bigger, and latency-sensitive applications require edge computing, perimeter-driven security strategies are gradually becoming inadequate in securing the heterogeneous and resource-strained infrastructures. Even with the robust protection paradigm presented by Zero-Trust Architecture (ZTA), current implementations tend to impose a heavy computational load, and can be based on centralized or blockchain-intensive architectures, not suitable to lightweight IoT implementations. To overcome those problems, the proposed structure incorporates edge-centric trust assessment, lightweight cryptographic identity authentication, and adaptive enforcement of the policy to support secure, scalable, and efficient distributed access control.

The presented multidimensional trust computation model dynamically assesses device integrity, behavioral patterns, contextual risk, and reputation metrics and is characterized by low computational complexity that can be used in edge environments. Analytical and comparative evaluations have shown better scalability, less latency, and better resistance to spoofing, replay attacks, insider threats, and lateral movement than more traditional centralized and blockchain-intensive solutions. The proposed architecture, which decentralizes its trust decisions to the edge layer and reduced the communications overhead, creates a coherent and resource-efficient Zero-Trust architecture that forms a viable base to the next generation of secure IoT-Edge-Cloud ecosystems.

Because the proposed model achieves linear-complexity, edge-local trust computation without reliance on consensus mechanisms, it is structurally positioned for deployment in constrained IoT environments where both blockchain-based and centralized ZTA models have been shown to be impractical.

9. LIMITATIONS

Despite the fact that the proposed lightweight Zero-Trust architecture offers a single and scalable security infrastructure in the IoT–Edge–Cloud continuum environments, there are a number of limitations that should be admitted.

First, the evaluation in this paper is primarily analytical, supported by a synthetic Python-based simulation (Section 6); it has not been validated through physical testbed deployment or large-scale real-world experimentation. Real-world application can uncover other latency limits, heterogeneity of hardware and software, other synchronization problems, and other network instability considerations to be optimized and empirically tested.

Second, the multidimensional trust computation model uses adaptive weighting factors that are predetermined to use device integrity, behavioral pattern, contextual risk, and reputation measurements. Although this is computationally easy and efficient, this method might be inadequate to reflect the fast-changing threat dynamics in highly adaptive adversarial systems, especially with the use of static or semi-static weight assignments.

Third, even though the architecture does not heavily use blockchain consensus to minimize computational cost, large-scale applications can still have gradual storage accumulation as a result of the accumulation of trust logs over time at the cloud layer. Scalability may then require efficient log aggregation, pruning techniques or compression techniques.

Fourth, the model supposes the moderate computational ability at the edge layer. Even lightweight evaluation of trust in even micro-edge cases can add observable processing overhead to ultra-constrained edge devices. Such environments may need hardware-aware optimization and adaptive trust computation scaling.

Fifth, Figures 1–4 are architectural and threat-model exposition diagrams, consistent with standard practice for presenting a system model and attack surface in systems and security papers, and are not intended to convey measured or simulated data. Figures 5–8 present results from a synthetic simulation using explicitly stated assumptions (Section 6.3) rather than hardware- or network-measured data, and Figure 9 (Section 6.3) now provides a timing-annotated sequence diagram of the trust-evaluation workflow using those same modeled latency values, closing the workflow-diagram gap identified in an earlier review; a sequence diagram and performance plots derived from physical-testbed measurement, rather than the modeled values used throughout this paper, remain a priority for future revisions (Section 10).

10. SCOPE FOR FURTHER RESEARCH

The proposed framework has several promising directions that can be enhanced with the help of future research:

1. **Empirical and Physical Testbed Validation (priority):** Discrete-event or network simulation (e.g., using OMNeT++ or NS-3) and physical edge-computing testbed deployment should be conducted to quantitatively validate the latency, computational overhead, and threat-detection results reported analytically and via synthetic simulation in this paper, including a sensitivity analysis of the adaptive weighting algorithm's parameters (η , w_{min} , w_{max}).
2. **Adaptive Trust weighting:** used with machine learning Machine Learning: With reinforcement learning, anomaly detection, or predictive modeling algorithms in place, adaptive adjustment of trust weights could be made based on changing attack behavior and contextual patterns to achieve greater adaptability and threat responsiveness.
3. **Light Hybrid Optimization: Alternative:** Investigations in future research might focus on lightweight blockchain options or directed acyclic graph (DAG)-based designs to find a balance between auditability, decentralization, and computational efficiency.

4. **Cross-Domain Trust Federation:** Building upon the architecture to leverage trust interoperability across administrative domains may allow federated IoT- Edge- Cloud ecosystems to collaborate safely and maintain decentralized policy enforcement.
5. **Energy-Aware Optimization of security:** To provide lasting performance, energy consumption modeling could be incorporated into the process of assessing trust in battery-powered and energy-limited IoT devices and determine their sustainability over time.
6. **Integration with Software-Defined Networking (SDN):** The proposed Zero-Trust architecture can be extended with SDN-based micro-segmentation and controllable network to further improve fine-grained isolation of traffic, orchestrated policy, and automatic threat containment.

REFERENCES

- Boubaker, S., Alsubaei, F. S., Said, Y., & Ahmed, H. E. (2023). Lightweight Cryptography for Connected Vehicles Communication Security on Edge Devices. *Electronics (Switzerland)*, 12(19). <https://doi.org/10.3390/electronics12194090>
- Cetintav, I., & Tahir Sandikkaya, M. (2025). A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs. *IEEE Access*, 13(February), 37703–37723. <https://doi.org/10.1109/ACCESS.2025.3546147>
- Das, A., Patterson, S., & Wittie, M. P. (2018). EdgeBench: Benchmarking Edge Computing Platforms. In *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)* (pp. 175-180).
- Dhanapala, I., & Bharti, S. (2024). *Toward a Performance-Based Trustworthy Edge-Cloud Continuum*. June.
- Feijoo-Añazco, A., Garcia-Carrillo, D., Sanchez-Gomez, J., & Marin-Perez, R. (2023). Innovative security and compression for constrained IoT networks. *Internet of Things (Netherlands)*, 24, 100899. <https://doi.org/10.1016/j.iot.2023.100899>
- He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, 2022. <https://doi.org/10.1155/2022/6476274>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, 25(12), 1–26.

<https://doi.org/10.3390/e25121595>

- Khan, I. U., Khan, F. M., Haider, Z. A., & Alturise, F. (2025). Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework. *Computers, Materials and Continua*, 85(3), 4307–4344. <https://doi.org/10.32604/cmc.2025.070189>
- Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., & Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. *Cybersecurity*, 7(1). <https://doi.org/10.1186/s42400-024-00212-0>
- Ma, Y. W., & Chiu, P. H. (2025). A novel risk-based access control engine in zero trust architecture for IoT network. *International Journal of Information Security*, 24(3), 1–14. <https://doi.org/10.1007/s10207-025-01030-2>
- Mangala, N., Rangwala, M., Aishwarya, S., Eswara Reddy, B., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2025). Differential Privacy for Secure Machine Learning in Healthcare IoT-Cloud Systems. *IEEE Access*, 13.
- Oh, J., Yu, S., Lee, J., Son, S., Kim, M., & Park, Y. (2021). A secure and lightweight authentication protocol for iot-based smart homes. *Sensors*, 21(4), 1–24. <https://doi.org/10.3390/s21041488>
- Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys and Tutorials*, 23(2), 1078–1124. <https://doi.org/10.1109/COMST.2021.3062546>
- Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, 10, 57143–57179. <https://doi.org/10.1109/ACCESS.2022.3174679>
- Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, 9, 28177–28193. <https://doi.org/10.1109/ACCESS.2021.3052867>
- Wang, B., Li, M., Jin, X., & Guo, C. (2020). A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities. *IEEE Access*, 8, 46373–46399. <https://doi.org/10.1109/ACCESS.2020.2979022>
- Wang, Y., & Wu, Z. (2023). Blockchain-Based Multidimensional Trust Management in Edge Computing. *IEEE Access*, 11(November), 122736–122748. <https://doi.org/10.1109/ACCESS.2023.3329126>

