Mathematics Research and Education Journal
Vol 10, No 1, Page 22-29, April 2026
Doi: 10.25299/mrej.2026.vol10(1).22109.
Internet of Things I Research Article OPEN ACCESS

Challenges for Security in IoT: A Comprehensive Approach with Mathematical Modeling, Zero Trust, and Solutions

Usman Ghani
Department of Mathematics, Faculty of Basic and Applied Sciences, Air University, Islamabad, Islamabad Capital Territory (ICT), Pakistan
usman.ghani@students.au.edu.pk

ABSTRACT

The Internet of Things (IoT) has transformed modern digital infrastructure by enabling intelligent connectivity among billions of devices across industries, healthcare, transportation, and smart homes. However, the rapid expansion of IoT networks has introduced serious security challenges, including weak authentication, unauthorized access, data interception, and limited device resources. This study proposes a comprehensive IoT security framework that integrates mathematical modeling, lightweight encryption, artificial intelligence, and Zero Trust Architecture (ZTA). Graph theory is applied to analyze trust propagation and identify vulnerable nodes within IoT networks, while dynamic trust scores are used to improve authentication and anomaly detection. Simulation results from a 25-node IoT environment demonstrate that the proposed integrated model achieves higher trust accuracy and detection rates with low computational overhead compared to traditional security approaches. The findings indicate that combining mathematical optimization with Zero Trust principles provides an adaptive, scalable, and efficient solution for strengthening IoT cybersecurity in modern interconnected systems.

ARTICLE HISTORY

Received 23 April 2025
Revised 1 February 2026
Accepted 23 April 2026

KEYWORDS

Internet of Things (IoT) 2; IoT Security Zero Trust Architecture (ZTA) 4; Mathematical Modeling

SUBJECT

Internet of Things Security, Zero Trust Architecture, Artificial Intelligence

1. Introduction

The Internet of Things (IoT) has become one of the most influential technologies in the modern digital era because it enables devices to communicate and exchange data automatically through internet networks [1]. IoT technology is widely implemented in various sectors, including healthcare, transportation, industrial automation, smart homes, and wearable devices[2]. Through integrated communication systems, IoT increases efficiency, automation, and decision-making processes in real time. The growing adoption of IoT devices has accelerated digital transformation worldwide and created new opportunities for innovation [3]. However, the rapid expansion of interconnected devices also introduces significant security concerns because sensitive information is continuously transmitted between devices, networks, and cloud systems.

One of the major challenges in IoT security is the limited capability of many devices. Most IoT devices are designed with low computational power, limited memory, and

restricted energy resources, making it difficult to implement advanced security mechanisms [4]. In many cases, manufacturers prioritize affordability and functionality rather than strong cybersecurity protection. As a result, IoT devices often contain vulnerabilities such as weak passwords, outdated firmware, poor encryption methods, and insecure communication protocols [5]. These weaknesses can be exploited by cybercriminals to perform malware attacks, unauthorized access, denial-of-service attacks, and data theft. Consequently, IoT systems become highly vulnerable to cyber threats that may affect both individuals and organizations.

IoT security challenges are further complicated because IoT ecosystems involve heterogeneous devices connected through different communication protocols and network architectures [6]. Sensors, gateways, cloud servers, mobile applications, and edge computing systems operate together in dynamic environments, creating complex interactions across multiple layers [7]. Traditional cybersecurity methods based on perimeter protection are no longer sufficient because attackers can exploit vulnerabilities from various points within the network. Researchers have proposed several security approaches, including cryptographic techniques, authentication systems, intrusion detection mechanisms, blockchain technology, and artificial intelligence-based security models [8]. Nevertheless, many existing approaches focus only on specific problems and often require computational resources that are unsuitable for lightweight IoT devices.

A promising solution for improving IoT security is the implementation of Zero Trust Architecture (ZTA). This approach follows the principle of "never trust, always verify," where every device, user, and communication request must be continuously authenticated before access is granted [9]. Unlike traditional network models that assume internal systems are secure, Zero Trust eliminates implicit trust and applies continuous monitoring and verification processes[10]. In addition, mathematical modeling contributes significantly to IoT security analysis by helping researchers evaluate trust relationships, identify vulnerable nodes, and optimize network performance. Mathematical approaches such as graph theory, probability analysis, and trust computation provide measurable methods for improving anomaly detection and communication reliability in IoT systems.

Artificial intelligence also strengthens IoT security through real-time monitoring and anomaly detection capabilities. AI-based systems can analyze network traffic patterns, recognize suspicious activities, and respond dynamically to emerging cyber threats. The integration of artificial intelligence, mathematical modeling, lightweight encryption, and Zero Trust Architecture creates a more adaptive and intelligent IoT security framework. Such integration supports the confidentiality, integrity, and availability of IoT data while maintaining computational efficiency for lightweight devices. Therefore, this study aims to develop a comprehensive IoT security framework capable of addressing modern cybersecurity challenges and contributing to the development of scalable, efficient, and resilient digital ecosystems in the future.

2. Methodology

This study adopts an analytical and simulation-based research design that integrates mathematical modeling with Zero Trust principles to evaluate IoT network security. The

methodology consists of four core components: (1) mathematical model formulation, (2) simulation setup and dataset configuration, (3) problem-solving scenario analysis, and (4) validation and ethical considerations.

2.1 Research Design

The research follows a quantitative analytical design supported by simulation experiments. It aims to quantify security parameters (trust, risk, and connectivity) through mathematical equations and validate them using simulated IoT data. The design is both conceptual (in defining the theoretical framework) and computational (in testing it using tools).

2.2 Mathematical Model Formulation

Three models are implemented to analyze IoT vulnerabilities and trust propagation:

Graph-Theoretical Model – The IoT network is represented as an undirected weighted graph G(V,E), where each vertex v_i∈Vrepresents an IoT device, and each edge e_ij∈Edenotes communication between devices. Edge weights w_ijreflect trust levels based on authentication frequency and successful data exchanges.

$$T(v_i) = \frac{\sum w_{ij}}{| E_i |}$$

where T(v_i)is the trust score of node i, and E_iis the set of its connected edges. Encryption Complexity Model – To assess computational efficiency, the encryption overhead C_eis defined as:

$$C_e = \frac{T_{enc} + T_{dec}}{S_{data}}$$

where T_encand T_decare encryption and decryption times, and S_datais the data size. This allows comparison between lightweight and standard cryptographic schemes.Trust Score Model – Dynamic trust scores are computed as:

$$TS_i = \alpha A_i + \beta C_i + \gamma H_i$$

where A_i= authentication success rate, C_i= communication reliability, and H_i= historical trust. Coefficients (α,β,γ) are empirically assigned based on sensitivity analysis.

2.3 Simulation Environment and Dataset

The simulations were implemented using Python (NetworkX 3.2) for graph modeling and MATLAB R2024a for trust and encryption computations. A simulated IoT network of 25 nodes was created, representing heterogeneous devices such as sensors, gateways, and controllers.

Each node exchanges data packets under different trust thresholds to test adaptive authentication mechanisms. Performance metrics such as average trust accuracy, latency, and computational load were recorded.

All dataset parameters and algorithms were generated synthetically to ensure controlled and repeatable experiments.

2.4 Problem-Solving Scenarios

The "Problem-Solving Scenarios" section has been restructured to separate problem identification from solution testing. The problem identification phase lists observed IoT vulnerabilities (e.g., weak authentication, data interception). The solution testing phase applies the proposed models under simulated attack conditions (e.g., replay or man-in-the-middle attacks) to measure model performance. This structured division provides a clear methodological justification and ensures logical consistency.

2.5 Ethical and Data Protection Considerations

Although this study uses simulated data, ethical standards for data integrity, privacy, and responsible AI use were maintained. No real user data were collected. The framework aligns with GDPR principles and NIST ethical AI guidelines, ensuring that the proposed methods promote privacy by design and minimize data exposure in IoT environments.

2.6 Zero Trust Architecture (ZTA) in IoT

Traditional perimeter-based models are inadequate for IoT environments. Zero Trust assumes that every device, user, and network must be verified.
Core Principle: "Never trust, always verify."
Mathematical Trust Score Model:

$$T(D_i) = \frac{A_i}{R_i + 1}$$

Where:

- A_i = authentication score
- R_i = risk score
- $T(D_i)$ = device trust score

Access Rule:

$$T(D_i) > \theta$$

Where θ is the trust threshold. Devices with scores below this are denied access.

2.7 Problem-Solving Scenarios

Scenario 1: Smart Home with Open Ports
Risk: Unauthorized remote access
Model:

Probability of a device d having open ports:

$$P(d) = \frac{o_d}{O}$$

Where o_d = open ports, O = total scanned ports

Solution: Use port cloaking, firewalls, and disable unused services.
Scenario 2: Data Theft from Wearables
Risk: Bluetooth sniffing and tracking
Model: Signal attenuation:

$$S = S_0 e^{-\alpha d}$$

Where:

- S = received signal strength
- S_0 = transmission strength
- α = attenuation coefficient
- d = distance

Solution: Encrypt transmissions and reduced range.

2.8 Recommendations

Adopt Zero Trust at the edge and device level
Implement secure development lifecycles
Use formal verification for firmware security
Deploy AI-based intrusion and anomaly detection systems
Conduct regular audits and device posture assessments

3. Results and Discussion

3.1 Results

The simulation was executed on a 25-node IoT network using the integrated Mathematical Modeling + ZeroTrustFramework.
Three performance metrics were measured:

1. Trust Accuracy (TA) – how precisely the model identifies reliable devices.
2. Detection Rate (DR) – percentage of correctly identified malicious nodes.
3. Computational Overhead (CO) – processing time per authentication request (in milliseconds).

Metric	Baseline IoT Security	LightweightEncryption Model	ProposedIntegrated Model
Trust Accuracy (TA)	72.8%	85.3%	94.6%
Detection Rate (DR)	68.5%	82.1%	91.7%
Computational Overhead (CO, ms)	15.8	13.2	14.1

The results show that the proposed model improves trust accuracy by 22% and detection rate by 23% compared to the baseline, while maintaining low computational overhead—an essential requirement for IoT devices.

3.1.1 Statistical Validation

To verify reliability, each simulation was repeated five times with varying trust thresholds. The standard deviation for trust accuracy remained below ±2.5%, confirming stability and repeatability of the results. A paired-sample t-test comparing baseline and proposed model outputs yielded $p < 0.05$, indicating a statistically significant improvement in detection and trust accuracy.

3.1.2 Comparative Analysis

To ensure objectivity, the earlier subjective scoring system ("9.5/10") has been replaced with data-driven evaluation metrics (accuracy %, delay, complexity).

Model	AI Integration	Zero Trust Layer	Avg. Detection (%)	Avg. Delay (ms)	Scalability Index
Baseline IoT	✗	✗	68.5	15.8	0.74
Lightweight IoT	✓	✗	82.1	13.2	0.79
ProposedIntegrated Model	✓	✓	91.7	14.1	0.88

Interpretation:

- The AI-based trust computation enhanced anomaly detection.
- Zero Trust enforcement reduced unauthorized access attempts.
- The model remained computationally efficient due to mathematical optimization in node ranking.

3.1.3 Visualization and Equation Explanation

Figure 5 (Trust Propagation Graph) illustrates node-to-node trust dynamics based on weighted edge values. The graph-theoretical equation was implemented to calculate each

node's trustworthiness. Nodes with lower weights correspond to potentially compromised devices, easily identifiable through visual clustering in the graph visualization. This helps automate risk detection and guide Zero Trust authentication responses

$$T(v_i) = \frac{\sum w_{ij}}{|E_i|}.$$

3.2 Discussion

The findings confirm that integrating Mathematical Modeling and Zero Trust Architecture (ZTA) significantly improves IoT security by combining analytical prediction and continuous verification.

- *Mathematical modeling quantifies trust propagation and identifies high-risk nodes through graph metrics, providing a measurable foundation for trust assessment.*
- *Zero Trust mechanisms then apply dynamic access control and continuous authentication, ensuring that even trusted nodes remain verifiable.*
- *Together, they form an adaptive, data-driven security ecosystem capable of responding in real time to anomalous network behavior.*

Compared with prior models that rely solely on static policies or heuristic thresholds, the proposed approach introduces a quantitative, verifiable trust mechanism supported by empirical results. While these outcomes are based on simulation data, they demonstrate the practical potential of mathematically guided Zero Trust strategies in real-world IoT systems.

4. Conclusion

IoT devices present unique security challenges due to their widespread adoption and limited resources. This paper introduces both theoretical and practical approaches, including graph theory for threat modeling, lightweight encryption for resource-constrained devices, and the Zero Trust framework for robust access control. These strategies aim to strengthen IoT defenses against evolving cyber threats. As IoT devices become more prevalent, securing them requires an interdisciplinary approach that integrates engineering, mathematical modeling, and policy-driven solutions. By combining these fields, we can create more effective and scalable security models for IoT networks. The proposed solutions provide a foundation for developing adaptive, efficient, and resilient IoT security systems.

References

[1] Y. Liu and M. Ye, "Application And Validity Analysis of IoT In Smart City Based On Entropy Method," *Applied Artificial Intelligence*, vol. 37, no. 1, 2023, doi: 10.1080/08839514.2023.2166234.

[2] P. M. Chanal, M. S. Kakkasageri, R. S. Pujar, G. S. Kori, and C. L. Chayalakshmi, "Regression-based context aware authentication scheme for IoT devices: cognitive agents approach," *Journal of Information and Telecommunication*, 2025, doi: 10.1080/24751839.2025.2600119.

[3] A. Vultureanu-Albişi, C. Bădică, and M. Ivanović, "eXING-IoT conceptual framework for explainability integration in next generation-IoT," *Conn. Sci.*, vol. 37, no. 1, 2025, doi: 10.1080/09540091.2025.2507180.

[4] A. Villafranca, K. Min Thant, I. Tasic, and M. D. Cano, "A deep learning-based IDS for IoT: model proposal and comparative study of dataset balancing techniques," *Journal of Information and Telecommunication*, 2026, doi: 10.1080/24751839.2026.2640249.

[5] A. F. Kineber, "Identifying the Internet of Things (IoT) implementation benefits for sustainable construction project," *HBRC Journal*, vol. 20, no. 1, pp. 700–766, 2024, doi: 10.1080/16874048.2024.2369462.

[6] I. Henriksson, C. Johansson-Malmeling, C. Gustavsson, and S. Johansson, "Experiences of using the internet among people with aphasia: challenges and opportunities," *Aphasiology*, 2025, doi: 10.1080/02687038.2025.2555865.

[7] Y. Na and N. Pun, "Internet as an ideology: nationalistic discourses, and multiple subject positions of Chinese internet workers," *Inter-Asia Cultural Studies*, vol. 24, no. 3, pp. 367–381, 2023, doi: 10.1080/14649373.2023.2209423.

[8] K. Alfredsson Ågren, A. Kjellberg, and H. Hemmingsson, "Access to and use of the Internet among adolescents and young adults with intellectual disabilities in everyday settings," *J. Intellect. Dev. Disabil.*, vol. 45, no. 1, pp. 89–98, Jan. 2020, doi: 10.3109/13668250.2018.1518898.

[9] P. G. Chiara, "The IoT and the new EU cybersecurity regulatory landscape," *International Review of Law, Computers and Technology*, vol. 36, no. 2, pp. 118–137, 2022, doi: 10.1080/13600869.2022.2060468.

[10] A. J. W. Andersen and T. Svensson, "Struggles for recognition: A content analysis of messages posted on the Internet," *J. Multidiscip. Healthc.*, vol. 5, pp. 153–162, 2012, doi: 10.2147/JMDH.S33418.