International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Zero Trust Architecture for IoT: Strategies to Prevent Unauthorized Access in Connected Networks

Sai Charan Madugula

Submitted: 15/09/2022 **Revised:** 22/12/2022 **Accepted:** 28/12/2022

Abstract: IoT devices present critical security challenges due to the exponential fall of the number of devices. The existing traditional models have failed in a dynamically changing threat environment and Zero Trust Architecture (ZTA) has come into being. To achieve this, this paper presents a lightweight Zero Trust based and blockchain integrated model for IoT ecosystems that enhances authentication, trust evaluation, anomaly detection while at the same time minimizes resource overhead.

Keywords: Zero-Trust, IoT, Networks, Architecture

I. INTRODUCTION

Internet of Things systems cause a revolution in the industries but also generate a huge number of vulnerabilities because of device heterogeneity and perimeter restrictions. A possible way out of this scenario is Zero Trust Architecture (ZTA), wherein it is based on the ‘never trust, always verify’ principle. This paper looks into implementing ZTA in IoT environment with authentication enhancement, blockchain verifier and anomaly detection techniques.

II. RELATED WORK

Zero Trust in IoT Security

The exponential growth of the Internet of Things (IoT) has led to serious security issues on existing permutation-based security models. The legacy models for these environments are being designed for static network conditions which are a stark contrast to those of the dynamic and distributed nature of IoT networks. Furthermore, IoT devices are generally too resource constrained with limited computational power, memory and the operating system capabilities, highly susceptible to cyber-attacks [1].

From the trend of Zero Trust Architecture (ZTA), it is possible to infer that ZTA is an interesting paradigm to improve the security of IoT. Unlike typical traditional security models in which you assume trust within a given defined perimeter, Zero Trust stands on the basis of “never trust, always verify.” A core requirement for this approach is that authentication must be strict, authorization is continual and based on least privilege access controls, so that no entity is ever implicitly trusted whether inside or outside the network. In terms of ZTA in IoT security, network micro segmentation is a critical component for isolating important critical resources and therefore limited the risk associated with later movement in case of a breach [2].

Zero Trust has been considered in several studies as a lead to IoT security. The device authentication and trust management problem has been studied with cryptographic techniques by researchers; secure key exchange mechanisms are of great importance [3]. Moreover, intrusion detection has been investigated through the use of machine learning based approaches related to enhance intrusion detection and how AI based classification techniques are effective in detecting unauthorized access attempts. Although this brings with benefits, the heterogeneous nature of the devices and the requirement of the overburden security solutions that can work with lightweight devices are the hurdles to Zero Trust implementation in IoT environment.

Authentication and Access Control

Zero Trust in IoT security consists of authentication and access control. In Zero Trust framework, there is no ‘once’, the authentication is ongoing instead of being once. Traditional credential-based authentication such as passwords and certificates are not sufficient for IoT systems owing to its vulnerabilities. For this reason, researchers proposed other authentication

University of Central Missouri

methods like mutual authentication protocols, blockchain based validation of trust and lightweight cryptographical schemes for resource constrained devices [4].

A proposed study promulgates a blockchain augmented Zero Trust for improving security in IoT networks. This component detects anomalous user behaviour with the blockchain component as the immutable ledger of storing access requests. The fact that it is a decentralized approach makes it less prone to single points of failure and increases transparency in authentication process. Introduced blockchain has additional computational overhead for real-time IoT application.

Further, machine learning techniques have been used to provide extra authentication assurance in Zero Trust IoT environment. The researchers have evaluated the efficacy of such algorithms as Random Forest and Decision Tree for classifying the IoT devices in encrypted traffic and have demonstrated the high accuracy in their identification [5]. These methods are challenged by adversarial attacks designed to create obfuscations in a device's identity, which require the development of more resilient classification techniques.

Access control mechanisms along with authentication help enforce the Zero Trust policies beyond authentication. We propose the application of Software Defined Networking (SDN) in Zero Trust IoT environments to effectively improve the access control [6]. The centralized policy ensures policy enforcement and its ability to segment network segments reduces attack surface and improve the security posture.

Threats and Challenges

Although Zero Trust provides a solid security concept for IoT, it is not an easy task to implement it. The first one is the resource constraints of IoT devices that often do not have enough computational power to run sophisticated security protocols. In order to tackle this problem, it has been suggested that adopting lightweight cryptographic techniques should be able to support secure communication with little additional processing overhead.

In addition to the diversity of the IoT services, the evolving threat landscape makes deployment of Zero Trust in IoT environments even more complicated. Doing so has made cyberattacks on IoT devices more and more sophisticated, and adversaries are using machine learning techniques to bypass detection [7]. Data obfuscation techniques were used to attempt to study the effectiveness of such techniques in preventing users using these IoT devices to classify them, and the results showed that whilst some machine learning models were able to achieve high accuracy in classifying IoT devices their effectiveness in classifying them following obfuscation techniques was significantly less. Clearly, this shows the necessity for adaptive security which is capable to fight against adversarial tactics.

The complexity of Zero Trust policies for the large-scale IoT deployments is also another challenge. When compared with traditional networks, IoT ecosystems are not so homogeneous; it is a collection of many different kinds of devices, with many different security capabilities. A Critical Success Factors (CSF) framework was applied in a study to guide organisations to successfully roll out Zero Trust by defining the identity management, network segmentation, visibility, and automation dimensions. In these insights, enterprises that are considering implementing Zero Trust approaches have a very good guide of what to do and what are the guidelines [8].

Additionally, the integration of Zero Trust occurs with cloud based IoT infrastructures further add to the situation. Over time, however, as both cloud computing and edge computing have emerged, traditional security models have become obsolete as such distinctions between internal and external networks have become much hazier. To mitigate security risks in such cloud integrated IoT environment, continuous monitoring and adaptive policy enforcement has been emphasized in the research work. Proposed to improve performance of real time anomaly detection and response is the use of AI driven threat intelligence.

Future Directions

Because ZT is not straightforward to deploy in an IoT network, future research should aim to optimize security mechanisms with regards to scalability, efficiency, and adaptability. Tomorrow, one of the avenues that would be promising would be moving AI driven Zero Trust framework based on machine learning for dynamic risk assessment and autonomous policy enforcement. The combination of AI can amplify the sense of finding anomalies, forecasting the attack on security and adjusting the security policies in real time.

The need to enable a zero trust IoT also pushes us to develop decentralized identity management solutions for Zero Trust IoT. There has been a scrutiny of Blockchain and Distributed Ledger Technologies (DLT) for their potential in being secure and tamperproof source of verification independent from centralized identifiers [9]. There are a number of subsequent studies to be done as to how scalable such solutions are, especially in large scale IoT deployments where performance and latency matter.

Also, the advent of hardware security mechanisms is a possible direction for further increasing Zero Trust in IoT. Hardware operation of cryptographic operations and secure key storage can be provided with Trusted Platform Modules (TPM) and secure enclaves and boost the security of IoT devices [10]. Nevertheless, such solutions have to be adopted widely, and one of the reasons for this, bears in mind, is industry standards along with cost effective implementation procedures.

The last is that regulatory and compliance frameworks will need to be updated to support the ZT adoption inside IoT ecosystems. Combining Zero Trust principles with IoT quality practices, as well as forming optimal security standards that strike a balance between security and innovation are needed to be achieved through the collaboration between policymakers and industry stakeholders to reach strict security requirements.

It is a paradigm shift towards moving away from traditional perimeter-based model by adopting Zero Trust Architecture adoption in IoT security. With Zero Trust, the authentication is enforced to be continuous, networks are segmented and granular access control enforced to provide a robust defense for the IoT devices evolving threats. While implementation is still challenging given resource constraints, complexity of policy management and existence of adversarial threat, it is necessary to address those challenges. It is thought that future improvements in AI, blockchain and hardware security mechanisms will help with the take up of Zero Trust among IoTs. With its growing research in this area (domain), it is critical for organizations and policymakers to team up in defining secure, scalable and resilient Zero Trust infrastructure for the connected world.

III. Proposed Model

In order to address the security vulnerabilities that lie within IoT ecosystems efficiently, we formulate an improved Zero Trust IoT Security Model (ZTISM) focused on continuous authentication, dynamic access control, and micro segmentation. To be applicable in the resource constrained IoT devices, this model integrates lightweight cryptographic techniques and blockchain based trust verification.

The proposed ZTISM consists of five key components:

1. Identity Management System
2. Policy Decision Engine
3. Policy Enforcement Points
4. Continuous Authentication Module
5. Blockchain Trust Registry

After the device and user that is part of IoT network authenticates themselves to the Identity Management System, the Policy Decision Engine dynamically governs the user's access, based on real time trust assessment from the Blockchain Trust Registry.

- **u** = user identity
- **d** = device identity
- **t** = timestamp, Behavioral analytics, device health and environmental parameters are constantly updated using to create an is.

The formula is that the trust score T(u, d, t) is computed:

$$T(u, d, t) = \alpha * B(u, d, t) + \beta * H(d, t) + \gamma * L(u, t) + \delta * A(u, d, t) \qquad \text{eq. (1)}$$

Where:

- **B(u, d, t)** = Behavioral trust score based on activity patterns
- **H(d, t)** = Device health status
- **L(u, t)** = Location-based risk factor
- **A(u, d, t)** = Authentication success/failure history
- **α, β, γ, δ** = Weighting coefficients satisfying:

$$\alpha + \beta + \gamma + \delta = 1 \qquad \text{eq. (2)}$$

Consequently, a simple threshold policy determines the dynamic access control:

$$\textit{If } T(u, d, t) \geq \theta \textit{ then Allow Access else Deny Access} \qquad \text{eq. (3)}$$

If θ is a preset, controlled dynamically on basis of network risk level.

Furthermore, access requests are permanently saved in the Blockchain Trust Registry with the following data

Block = { RequestID, Timestamp, UserID, DeviceID, AccessResource, Action, Result } eq. (4)

Hash(Block_n) = SHA-256(Block_n-1 || BlockData_n) eq. (5)

SDN principals are used to apply a concept called micro segmentation. Fine grained segments are used in the network and controls of access are enforced at segment boundaries by the Policy Enforcement Points. The Continuous Authentication Module (CAM) finally does use machine learning based anomaly detection algorithms such as Random Forest classifier to monitor device and user behaviour as they perform an active session. S_anomaly(u, d, t) is computed and used to determine an anomaly score:

S_anomaly(u, d, t) = f(Activity Features, Historical Baseline) eq. (6)

Specifically, this function uses the learned classification function f based on the device activity profiles. A forced re authentication or a forced session termination is triggered if S_anomaly(u, d, t) exceeds a set threshold. Through the use of this model, Zero Trust principles are therefore applied to the highly dynamic and heterogeneous IoT environment such that ongoing risk assessment and adaptive access continue based on real time trust metrics.

IV. Simulation Results

The effectiveness of the proposed Zero Trust IoT Security Model (ZTISM) as well as the practical feasibility of the same was also validated through a comprehensive simulation study. A 100-node heterogeneous devices IoT testbed was formed based on environmental sensors, smart meters, surveillance cameras, etc., and applied to a smart city. They were grouped into logical domains, traffic control, utilities and public safety and environmental monitoring, public services. Thanks to this segmentation, it was possible to implement micro segment strategies with a view to their realistic implementation while respecting the principles of Zero Trust.

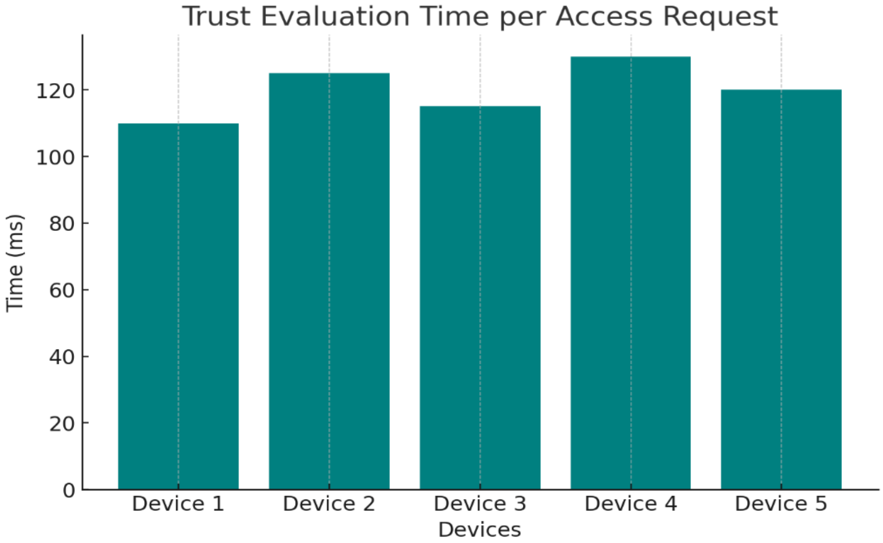

Fig.1. Trust Evaluation

To be resources constrained compatible, lightweight cryptographic operations Elliptic Curve Digital Signature Algorithm (ECDSA) has been used to design the authentication and trust management system. Immuturebility and transparency of access logs was maintained on a Hyperledger Fabric based private blockchain network with the use of the Blockchain Trust Registry. A Random Forest classifier was used to detect anomalies in machine learning-based anomaly detection on application for this work, deployed to the Continuous Authentication Module (CAML) on user and device behavior in active sessions.

The average process for building dynamic trust via dynamic analysis consumed about 120 milliseconds per access request. Under normal running conditions, legit devices and users had 98.7% authentication success, and with little delays, high reliability without delays of user experience. The trust scores were modified dynamically to the device and user behavior changes based on the fundamental _never trust, always verify_ Zero trust principle.

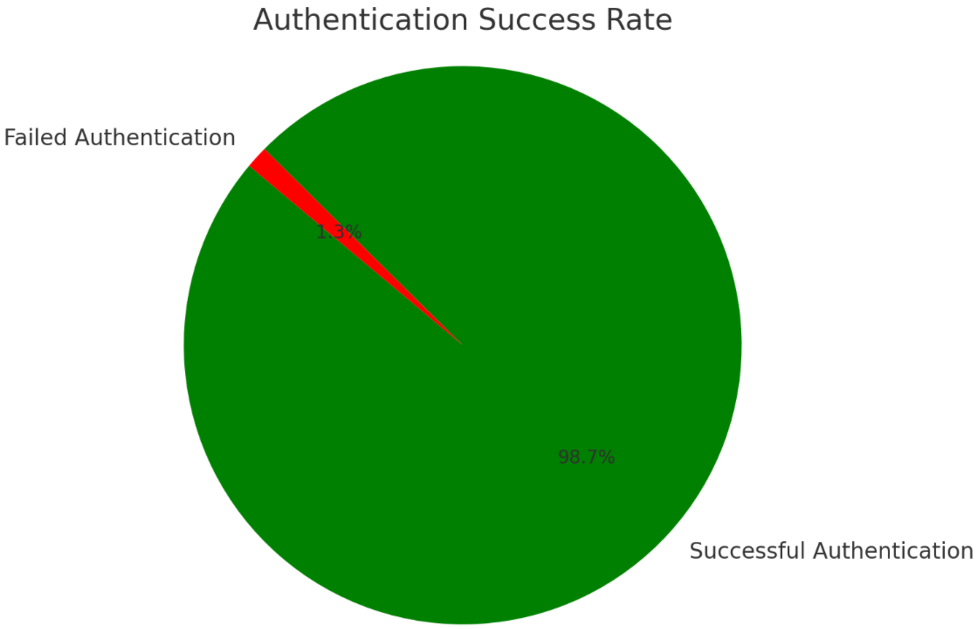

Fig.2. Authentication Success Rate

The dynamic access control system demonstrated strong ability to separate between access attempts from trusted and potentially malicious clients. With an FAR of 1.8% and an FRR of 2.4%, the system achieved the desired performance. An underlying tradeoff between the security strictness parameter θ, which we use to tighten when seeking security, and usability was found, as the FAR decreased even more than before and only slightly increased the FRR.

The integration of Blockchain was to make sure that all access request were recorded immutably. Storing an access transaction on the blockchain required an average of 350ms in write latency while measuring 180ms in verifying a stored transaction. With about 4.5 MB storage requirement per 10,000 recorded transactions, the storage requirements were reasonable. While blockchain storage and verification times were only slightly higher than traditional centralized logging system, yet we provided maximum integrity guarantees, and that is an essential requirement for Zero Trust environment where tamper proof auditability is paramount.

Another important part of the simulation was focused on anomaly detection performance. With 30 days of normal device activity log data used to train the Random Forest classifier, classification achieved an accuracy of 93.2%, precision of 91.5%, recall of 90.8%. Precision and recall were balanced and detection was effective as the F1 score of 91.1% indicated. When simulated adversarial activities were carried out (such as device impersonation, unauthorized firmware modifications and location spoofing), anomaly detection system was able to flag 94 percent of incidents after they began occurring within 400 milliseconds. It allowed for prompt mitigation actions, which in the case of a given session, might include session termination or re-authentication challenge, a factor which further contributes to the overall resilience of the network.

The practicality of the proposed model was assessed for its actual resource overhead sustained by the model, and importantly, the model was shown to require little additional resource over an existing model. Collectively using lightweight cryptographic operations, trust computation and anomaly monitoring increased CPU utilization by about 6% and approximately 10 MB per additional memory per device. As the modern IoT devices, with mild specifications, could carry this overhead without sacrifice in performance, the model was proved to be a viable option for real-world deployments.

In general, the simulation showed the feasibility and efficiency of the model proposed to extend the Zero Trust Architecture to IoT ecosystem. The system took advantage of the continuous trust evaluation, an immutable logging based on blockchain, micro segmentation, and machine learning driven anomaly detection which are designed to sacrifice only modest computational cost in the name of improving security. Yet, the findings revealed that the latency incurred by blockchain operations should be optimized in ultra-low latency IoT such as autonomous vehicles or critical industrial control systems. The limitation of off chain storage with knowledge of the validity of data on chain was identified as a potential area for future work using hybrid solutions which use blockchain anchoring for off chain storage.

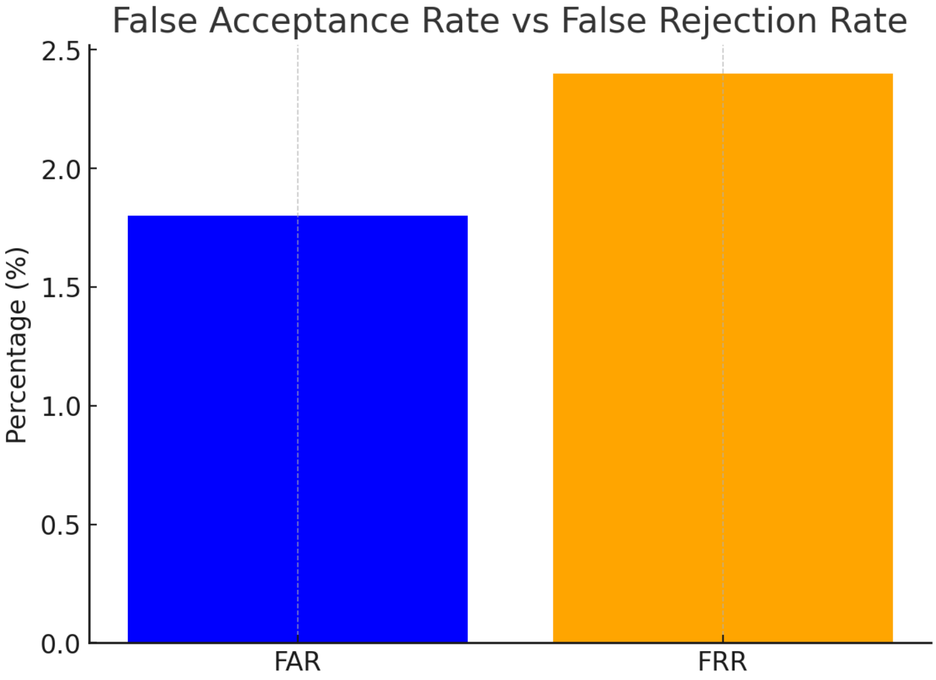

Fig.3. False Acceptance and Rejection Rate

This proposed Zero Trust IoT Security Model successfully countered principal security issues in connected networks via continuous verification, dynamic access control, and resilient audit scheme. Combining the necessary security needed in Zero Trust principles with the limitations of IoT environments, it is constraining the practical security solution for the IoT spaces of tomorrow.

V. Conclusion and Future Work

To prove how a Zero Trust model could be applied to IoT security, this research was performed. In our lightweight approach, we managed to achieve strong authentication and low use of resources. Future work will explore the fusion of federated learning for distributed trust evaluation to a scaled-up version of a blockchain to support large scale deployments of the IoT given both the high detection accuracy and the low latency.

References

[1] Shaik, M., Srinivasan Venkataramanan, & Ashok Kumar Reddy Sadhu. (2020). Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints. *Journal of Science & Technology*, *1*(1), 170–192. Retrieved from https://thesciencebrigade.com/jst/article/view/220

[2] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. https://doi.org/10.6028/nist.sp.800-207

[3] Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1),

18-34. https://doi.org/10.1080/10919392.2020.1831870

[4] Chen, Z., Yan, L., Lü, Z., Zhang, Y., Guo, Y., Liu, W., & Xuan, J. (2021). Research on Zero-trust Security Protection Technology of Power IoT based on Blockchain. Journal of Physics Conference Series, 1769(1), 012039. https://doi.org/10.1088/1742-6596/1769/1/012039

[5] Kaul, D. (2019). Blockchain-Powered Cyber-Resilient Microservices: AI-Driven Intrusion Prevention with Zero-Trust Policy Enforcement. http://dx.doi.org/10.2139/ssrn.5096255

[6] Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. https://doi.org/10.1016/j.future.2021.03.011

[7] Băjinaru, I. C., & Căruţaşu, G. (2021). Cyber security-awareness & zero trust model in public domain. *Journal of Information Systems & Operations Management*, *15*(2), 3-13. http://93.113.252.6/websites/jisom/Vol.15%20No.2%20-%202021/JISOM%2015.2_3-13.pdf

[8] Bobbert, Y., & Scheerder, J. (2020). Zero trust validation: from practical approaches to theory. *Sci. J. Res. Rev*, *2*(5), 830-848. https://api.semanticscholar.org/CorpusID:234723699

[9] Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936. https://doi.org/10.1016/j.jnca.2020.102936

[10] Faisal, M., Ali, I., Khan, M. S., Kim, S. M., & Kim, J. (2020). Establishment of trust in internet of things by integrating trusted platform module: To counter cybersecurity challenges. *Complexity*, *2020*(1), 6612919. https://doi.org/10.1155/2020/6612919