electronics

MDPI

Article

Zero-Tolerance Security Paradigm for Enterprise-Specific Industrial Internet of Things

Usman Tariq

Department of Management Information Systems, College of Business Adminstration, Prince Sattam Bin Abdulaziz University, Al-Khraj 16278, Saudi Arabia; u.tariq@psau.edu.sa; Tel.: +966-11-588-7080

Abstract: The complex industrial environment of the 21st century is equipped with the Internet of Things platform, with the objective of real-time operational visibility, improved device management and predictive maintenance. To unleash the focused importance of its policy, a secure connectivity must be realized through a range of existing and dissimilar devices and data sources. During the conceptualization phase, the authors aimed to compel the following: (a) that restriction of access should be based on the presence of unexpected device actions that may point to a security breach, and (b) ensure the safety of the system by constant tracking of connected devices and data. In this paper, a policy-driven, zero-trust defense model is proposed to address numerous vulnerable entry points, validate device access to legitimate enterprise functions, quarantine unsecure devices, and trigger automated warnings and policy validation for hardware, software, network connectivity and data management. To handle active scanning, bots, passive auditing, outbound threat management, and device interconnections, an experimental environment was put up. This environment provides holistic visibility and a persistent view of all resources, including those that were previously unknown. A steady stream of reliable and authenticated data has helped to develop and adjust a scalable implementation strategy by avoiding recognized anomalous traps. Actual data was aggregated and analyzed to assess the proposed methodology. Comparative analysis of 'device exposure view, attack path analysis, controlled view of devices, comprehensive vulnerability evaluation, and effective communication of cyber risk' has proved the effectiveness of the proposed methodology.

Keywords: Industrial Internet of Things (IIoT); risk management; zero-tolerance security framework

check for updates

Citation: Tariq, U. Zero-Tolerance Security Paradigm for Enterprise-Specific Industrial Internet of Things. *Electronics* **2022**, *11*, 3953. https://doi.org/10.3390/electronics11233953

Academic Editors: Umer Farooq, Najam Hasan, Ali Kashif Bashir and Olivier Sename

Received: 21 September 2022
Accepted: 21 November 2022
Published: 29 November 2022

1. Introduction

Regardless of industrial scope (e.g., automotive, energy, oil and gas, etc.), by exploiting next-generation technologies (e.g., multiple connectivity features, artificial intelligence systems, energy, and process optimization algorithms), IIoT will be able to standardize any non-identical process data and geographically scattered installations. Conflicting with the traditional method of the industry, in which a hardware-based assembly was equipped with ubiquitous communication, Industry 4.0 presented elastic systems whose utilities are not destined to specific hardware but are scattered all over the network.

The propagation of smart nodes has seen an escalation in security exposures and the apprehension of security adaptability. IIoT users have the de facto obligation of safeguarding the system and to deliver precautionary processes when security problems arise. A few generic security issues are vulnerable components, abnormal management processes, legacy control systems, insecure protocols, unused functionality, and hyper-connected data dissemination. One of the major concerns with IIoT is the disintegration of equipment and the diversity of standards, rules, and frameworks. The interoperability of IIoT entities can be hampered by the ever-changing usage of IIoT techniques like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol).

The primary objective of the proposed methodology is to ensure:

(a) The ‘zero trust network architecture’ by enforcing a flexible and real-time vulnerability scanning on edge and intermediate nodes (i.e., sensors, actuators, PLCs (programmable logic controllers), routers, gateways). Implementing a zero trust framework allows stakeholders to update their IT security, run their hybrid operations, and access the full array of IIoT apps without fear of compromise.
(b) Aggregate and disseminate required information (i.e., IP address, device physical location, system operation and production data, SCADA data, etc.).
(c) Measure and verify the reliability, precision, integrity, quality and extensibility of the acquired data.
(d) Respond to incidents by enforcing policies. The level of trust that should be allowed was determined with the use of in-depth and comprehensive knowledge about the operational identity and device settings.

The devices that make up the Industrial Internet of Things are often a part of a larger, more complex network that provides advantages to businesses of all sizes. Because of the interconnected nature of these devices, it is simpler to gather information, analyze that information, and then automatically react to changes in the surroundings. Often, these devices are involved in a huge data exchange, yielding a network that uniformly delivers data at very high speeds across all nodes. Most IIoT devices function in an unattended environment, making it more likely that an intruder may get access to them whether in person or remotely. As a direct consequence of this, intruders may get vital controls via data transmission by covertly eavesdropping to the inter-device transmission, since the vast majority of IoT devices employ wireless connectivity.

In this paper, the author′s goal is to incorporate security into IIoT nodes at all points in the network. This is done with the intention of preventing anomalous exposures from jeopardizing the security of the whole setup by forming a circle of trust. Projected contribution determines the impact of privilege escalation, broadcast of malicious executables without detection, proxy logon, and discourage maintaining stealth while being a malevolent node (i.e., unmanaged, non-instrumental, and rogue). The experimental evaluation highlights the importance of combining rules and behavior-based analyses with coherent clusters of nodes to identify known and unknown threats more accurately and in a deeper context. The countermeasure that was implemented has been modified and improved on a regular basis to:

(a) analyze attack mapping in terms of behaviors and interactions,
(b) improve the time and duration of detection and management of attacks,
(c) keep track of information on the attacker and the victim,
(d) adjust policy measures to accumulate metric details, and
(e) proactively modify the risk assessment that has proven useful in preventing future risks.

The rest of the paper is organized as follows: Section 2 sets out related work. Section 3 outlines the security challenges for devices and data that are associated with each changing infrastructure landscape. Sections 4 and 5 present the proposed framework and performance assessment of the zero trust security model. The conclusion underlines the importance of eliminating blind spots, the complete visibility of the network and the impact of increased collaboration.

2. Related Work

Hassanzadeh et al. [1] proposed a ‘spiral attack model’ to capture cyber breaches against various levels of attacks in IIoT environments. The scheme illustrated the usual time obligatory for concluding each phase (i.e., identifying targets, compromising targets, and launching internal and external exploitation) of the IIoT attack lifecycle. The authors also presented a machine learning taxonomy methodology to record security warnings at IIoT attack levels and architectural layers. The classification of alerts has been helpful in prognostic analysis systems to estimate combative choices and potential next attacks, which can help moderate threats faster and disrupt the chain of destruction.

Bassma et al. [2] presented an IoT Conjunction threat anomaly catalogue and offered a standardized risk assessment system for a cohesive 'Automated Risk Assessment System' (ARAS) based on ISO/IEC 27030 procedures. The authors failed to present a valid evaluation and testing framework (e.g., simulation outcome) to support their theory.

Hussain et al. [3] combined Physically Unclonable Function (PUF) hardware consuming FPGAs, together with a multi-layer method associated with cloud computing with an aim to enable the development of an enhanced multi-layer validation mechanism. The result of the evaluation of the proposed program provided a significantly higher load of requests to validate nodes using a built-up architecture in less than a second. This functionality has allowed IIoT configuration to gain low network latency with improved ACK time.

Aparna et al., [4] focused on information dissemination issues within the IIoT-compatible system and proposed a distributed model based on the Blockchain "DMIIoT". The projected prototype makes use of a safe P2P network, in which all nodes are free to communicate data with one another to promote trust via openness and high-quality information sharing. The authors compared DMIIoT to leading-edge methods using factors such as processing capacity, stability, energy administration costs and communication times. The results of the evaluation show that the Blockchain-based DMIIoT reduces the latency associated with the typical Smart Grid (SG) system.

Table 1 provides a comparison of currently available IoT (IIoT/IoMT (internet of medical things)) security procedures, while Table 2 details the most critical vulnerabilities present in IoT (IIoT/IoMT) security protocols.

Table 1. Comparison of existing IoT (IIoT/IoMT (internet of medical things)) security mechanisms.

Method	Layer	Description	Focused Issues
Security and privacy framework [5]	Application	To deal with failure points, privacy and security issues, Interplanetary File System (IPFS) cluster nodes have been integrated into the consortium Blockchain environment.	A framework has been established to ensure safety and control of devices. Applied technique does not promise effectiveness for real-time application systems, specifically when system is dense due to large number of peers.
Mitigating cyberattacks [6]	Application and Network	Performance evaluation of cryptographic authentication protocols, and critical review of IoMT network security vulnerabilities.	Rahman et al. proposed a novel mechanism to evade the impact of DDoS, Jamming, Node-Injection and Node-Hijacking associated with healthcare devices. Proposed method did not emphasize post-attack device behavior and how to subtract insecure code from victim nodes.
Multiuser physical layer authentication [7]	Physical	SVM-PO based self-directed parameter optimization to find out the best channel matrix aspect.	Du et al. demonstrated the security authentication mechanism using matrix channel estimation. Presented method did not discuss the perseverance of deployment and node location factor, as location identification can be a vital factor to authenticate egress and ingress nodes.
Optimal Resource Allocation [8]	Application and Network	Ensuring the channel security and applying convolutional neural network (CNN) to guarantee optimal channel state.	Goswami et al. simulated a novel technique to diminish the loss of network resources and identify data-driven vulnerabilities. Allocating resources proved its usefulness to balance the load and improve system performance. Unfortunately, proposed method lays the emphasis on QoS (quality of service) relevant to network communication and did not effectively consider energy consumption as a considerable data point during resource allocation.

Table 2. Key security breaches in IoT (IIoT/IoMT) security protocols.

Security Attributes	Xiong et al. [9]	Li et al. [10]	Nguyen et al. [11]	Echeverría et al. [12]	Kim et al. [13]
Dynamic authentication	Yes	No	Yes	No	No
Anonymity	No	No	No	No	No
Strong encryption	Yes	No	No	Yes	Yes
Forward secrecy	Yes	Yes	No		No
Autonomous mechanism	No	No	Yes	Yes	No
Secure mutual user/device authentication	Yes	No	Yes	No	No
Secure user/device registration	No	No	Yes	No	Yes
Device impersonation attacks	No	Yes	Yes	No	No
DDoS attacks	No	Yes	No	Yes	No
Stolen device verify attacks	No	No	Yes	No	No
Wormhole attack	No	Yes	No	No	No
Node malfunction attacks	No	No	No	No	No

Taheri et al. [14] presented a novel malware detection scheme named FED-IIoT that includes a variety of independently distributed learning models that are exactly like one another. The author customized and revised the Byzantine defensive method on Krum and Medium, then used it to defend against this kind of exploit and validated the efficacy of his strategy. To demonstrate the efficacy of the proposed algorithm, the author carried out a comprehensive series of tests on three separate IoT datasets, each of which used a unique collection of attributes. These tests validated both the attack and defensive mechanisms. The suggested technique did not apply robust supervised techniques based on a GAN model or analyze the IIoT data's unusual behavior, notably for varied streamlining Android apps. The authors vowed to follow up with research that focuses on rigorous data consolidation tactics, such as data processing, to enhance GAN and federating algorithms in IIoT systems.

3. Security Authentication and Data Protection Challenges

3.1. Identification Challenge

There is the notion of digital distinctiveness to nodes per se, which plays a fundamental role in the future of IToT integration. If enterprises require the benefit of connected sensing nodes, then protection should be end-to-end. The integrated equipment must be an accredited entity to conduct process and relay any desired commands.

3.2. Hardware Shareware Detachment

Another observed reproach in the IIoT network was a disengagement between hardware and shareware (i.e., public domain software) security. It is recommended that edge nodes have appropriate hardware IP privileged nodes that can switch to secure access rights without the participation of that process fetching any sort of security hazard. This objective should be achieved in consideration of (a) moderate difficulty of IToT systems; (b) predefine and follow-up security practice policy with resilience and lifecycle provisioning; (c) classify data with information modeling in an environment where all sensing, relay and sink nodes are expected to be hyper-connected and controlled by the base station.

It is worth highlighting that connecting a mobile or new device securely necessitates: (a) node authentication and authorization, (b) a secure bot to verify the integrity of installed firmware software (i.e., hardware-controlling software), and (c) a centrally accessible privilege matrix.

3.3. Intensity of IIoT Infrastructure SECURITY

The performance ratio of applied defense models varies in consideration of the following scenarios:

(a) Does information (i.e., during aggregation, processing, communication, and storage) need to be private (at edge, intermediate, gateway and base station)?
(b) How many levels (i.e., sensing node, sink node, base station) of an audit will be conducted to obtain a desired data trust level?
(c) What is the acceptable threshold of latency (i.e., in terms of data, network, and anomaly alerts generation)?
(d) What is the applicable Access Control Policy selection and follow-up criteria to revoke a blacklisted device or data stream?
(e) How often does firmware on IIoT devices need to be patched/updated, and what is the 'access control right' permission level of devices that need to be functional throughout an ongoing process?
(f) What necessary preliminary steps must be taken before and after devices are decommissioned? This consideration is vital to diminish the risks associated with threats such as spoofing, software tempering, repudiation, denial of service, and regulatory non-compliance.

4. Proposed Framework

A functioning IIoT environment includes features such as (a) effective and efficient device management; and (b) software and node integration. This implies that the applied framework should be accountable for alerts if an attempt is made to connect or install unauthenticated software. In this sense, the alert refers to data that the system provides to the IIoT ecosystem; (c) the management of security-sensitive data; and (d) data sharing with direct and distinct revocation.

Figure 1 illustrates the anomaly identification and tolerance process of the proposed framework that is explained in detail in subsequent steps (1 to 7).

Step 1: Authentication and Authorization of Devices

Authentication is the practice to recognize nodes. For MQTT [15], the authentication progression is to ensure that the node's patron ID/IP is legal, i.e., that the identity checksum belongs to the node in question. Whereas the authorization provides a method for assembling a specific node to some permissions.

For this reason, the proposed scheme adapted and implemented the X.509 protocol described in IETF RFC 5280 [16]. Certificate X.509 is built into many protocols, such as the secure socket layer, which is essential for the protection of server and network subdomains. Protocol considered the certificate as a public key with embodied metadata. The Distinguished Encoding Rules (DER) were adopted as an encoded public key, while the Public Key Infrastructure (PKI (RSA-AES)) [17] meant an universal modus for distributing, practicing, managing and removing X509 certificates.

Pseudo code (a-to-e) took the assumption that certificate-based authentication identifies a participant, computer, or device before giving access to a resource, network, or application. The system used 'group rules and privileges' to limit user and device access to data processing and networking resources. Consequently, only approved users will be able to access the necessary information. By combining it with other Conditional Access features such as multi-factor authentication, the capability will give an even greater degree of security for operational devices. It supports granular authentication policies and attributes OID (object identifiers) from the certificate issuer which is used to enforce MFA rules. In its current form, the proposed method does not allow for the provision of additional parameters, such as the operative-ruleset, key-id, or issuer, to associate certificates with node accounts.

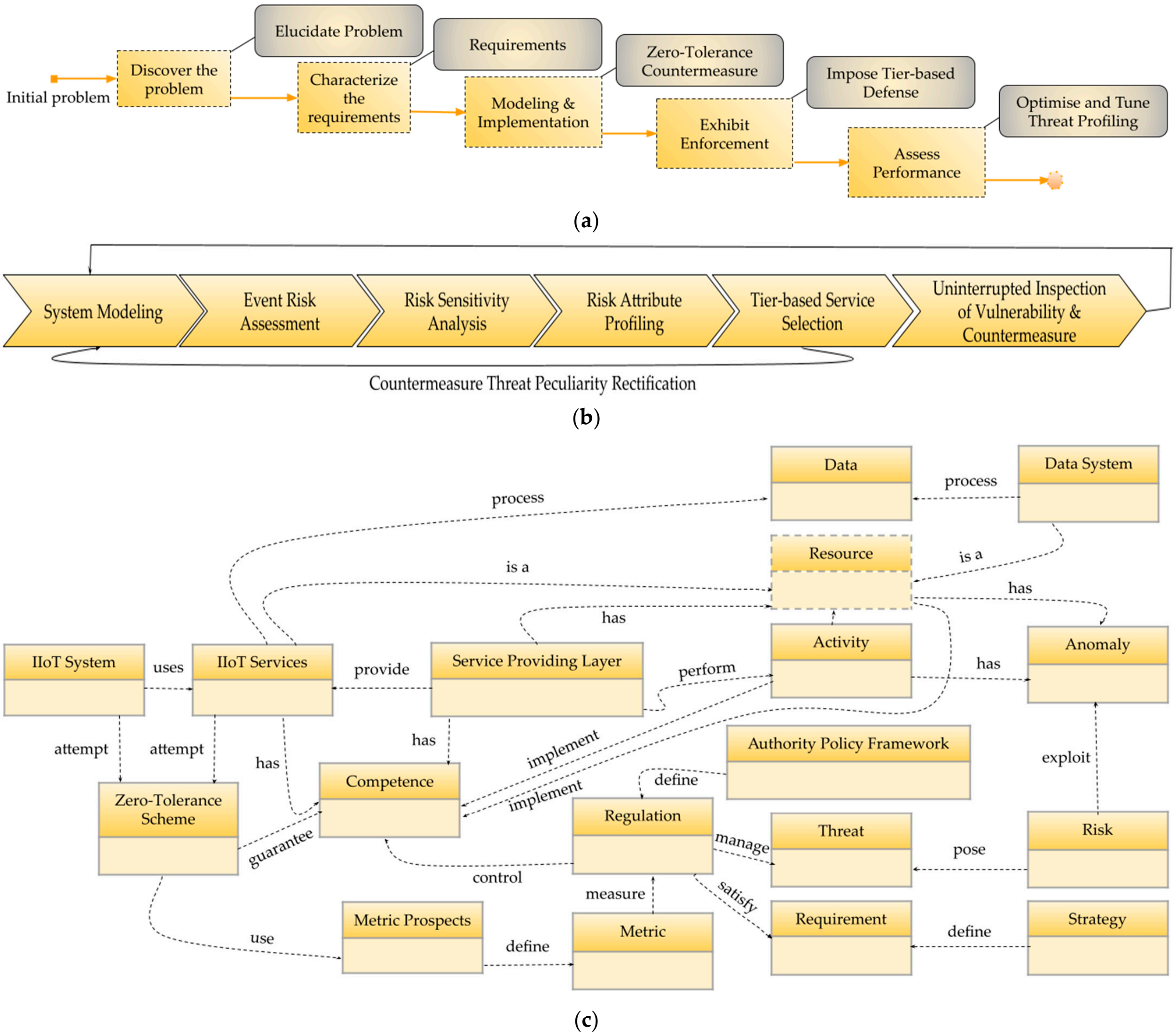


Figure 1. Leveraging Zero-Tolerance Security Framework. (**a**) Outline of the framework for design science study. (**b**) Uninterrupted Perceptible Risk Management. (**c**) Model integration.

Step 2: Device Profiling

Device profiling allows the competent authority to collect device type and OS data by examining packets that are passed through IoT nodes positioned in the network. In the proposed framework, the user of the device is eligible to make a profile of the device, which can aid in diminishing the effect of *side-channel attacks (SCAs)*. SCA tolerates secret key retrieval with a particular power trace, sanctioning the evasion of many re-keying counter procedures aimed at limiting the number of traces a malicious entity can secure for a given key. Furthermore, the author has applied 'constant time function' to encapsulate data without revealing the forensic data outcome to the anomalous entities.

As indicated in Table 3, device profiling played a vital role in the segmentation of the network. By isolating Internet of Things nodes from the diversified internet infrastructure, network segmentation prevented data from flowing in the wrong direction and contained insider threats. To improve the effectiveness of profiling, a *Configuration Management Database (CMDB)* was integrated into the accumulated dataset. The CMDB provided a resource to understand the significant enterprise resources (ICT (internet communication technology) devices) and their links. The core functions of the CMDB include, but are not limited to, compliance functions, federated data sets, IToT provision mapping, and device and process access control.

Pseudo Code 1 (a): Connection to the server using session token

```
var session = provision.getSession();
var nodeId = session.node_id;
var MAC = session.token;
var parameters = {nodeID, MAC};
```

Pseudo Code 1 (b): Alert generation

```
var discourse = "...";

var alert = {
type:  "indicator",
body:  "alert_ID",
delay:  {
include_to_history:  01,
negotiation_id:  messge._id
},
indicator:  01
};

var destination_node-Id = 07;
attempt {
alert.id = indicator.send(destination_node-Id, alert);
} latch (m) {
if (m.node_indicator === 'indicator_Not_Linked_Error') {
}
}
```

Pseudo Code 1(c): Ping node by ID

```
attempt {
alert.ping(nodeId, utility (error) {
if (error) {
// no syn-alert received
} else {
// syn-alert received from node
}
});
} latch (m) {
if (m.ID === 'indicator_Not_Connected_Error') {
// not connected to node/server/basestation
}
}
```

Pseudo Code 1(d): Access Node List

```
try {
node.alert.register.get(method(node_list) {

});
} latch (m) {
if (m.node_indicator === 'indicator_Not_Connected_Error') {
}
}
```

Pseudo Code 1(e): Add new node to register list

```
var nodeId = 56;
attempt {
node.alert.register.get (nodeId, method() {

});
} latch (m) {
if (m.node_indicator === 'indicator_Not_Connected_Error') {
}
}
```

Table 3. Sampler Profiling Data Set.

DID	Interface Name	IP Address	Interface Type	DAPM	VLAN Identifier	SCAs
1	Android	10.0.13.2	Dynamic	Disabled	13	Timing attack, Electromagnetic attack, Simple and Differential power analysis
2	Dynamic	10.0.12.2	Dynamic	Disabled	12	
3	Management	10.0.11.2	Static	Enabled	11	
4	Ubuntu	10.0.10.2	Dynamic	Disabled	10	

It is important to emphasize that a SCA obtains data from a chipset or subsystem in order to function properly. The module has examined and assessed a wide variety of the entity's physical features. It was observed that if the flaws are discovered, it posed a risk to cryptographic components. Several different side-channel analysis methods have been successful in breaking computationally robust cryptography and extracting the data that was encrypted. The threat to SCA is a major concern for hardware platforms. An adversary may break the intended encryption algorithm by leaking power physically or by analyzing electromagnetic (EM) signals from a profiling device. Both of these methods are potential methods of attack.

Step 3: Denial of unsecured devices

Enterprise IoT nodes can be characterized as information technology nodes. A real time ‘index (search engine)’ was created to log current and resumed IoT nodes with a purpose to update and retrieve device data from CMBD. A multipurpose grouping search algorithm (Genetic Algorithm (GA) [18]) periodically scanned the predefined portion of cluster nodes to register any variation in the device relevant register. The grouping of IoT devices was programmed according to several features, including the packet payload arrival rate, the Discontinuous Receiving Mechanism (DRM) model, QoS prerequisites, and the agility model. The GA algorithm models were optimized with the considerations, such as device mobility, communication, consistency, service interval, and latency in sensor data communication.

$$Confidence = \frac{f(\rho\text{-}value)_x(\rho_{hypothesis})_d}{\sum_{y-1}^{n}\left(f(\rho\text{-}value)_i(\rho_{hypothesis})_y\right)} \tag{1}$$

The probability of hypothesis was investigated through independent segmentation of the devices. Where ‘*f*” represents the function associated with implied sequence ‘*i*’ to a hypothesis ruleset ‘*y*’ and ρ refers as ‘variable dependences. By applying threshold to confidence equation,

$$\rho_{threshold} < \rho_{obtaiined\_score} \tag{2}$$

Score from all evaluated devices (J_y) was recorded to segment as

$$J_y = \sum_{y=1}^{m} j_x \tag{3}$$

Thus

$$\rho_{overall} = \rho_{segment}\rho_{Hypothesis}\rho_{ruleset} \tag{4}$$

The security of the integrated devices was assessed based on the following characteristics:

(a) Insecure system devices that operate on nodes which are connected to the network.
(b) The under-evaluation architecture only used the hardware components that are capable of Zigbee communication protocol usage [19].
(c) Router that is eligible to connect to remote web edges.
(d) In a situation in which it is difficult to keep track of the software, outdated firmware components were investigated.
(e) A lack of ‘physical reinforcement’ that might potentially create an impending cyber-attack or seize native control of built-in Internet of Things devices.

Taking into consideration the aforementioned assertions (a–e), a device profile is a collection of characteristics that, taken as a whole, characterize the computer’s hardware and software configuration. The author considered (but was not limited to) the device profiling feature as: node regulatory templates, settings for risk that are already specified, settings library to access all the options that are accessible, information and derived ruleset for adopted platform by each networked nodes, device restrictions (i.e., permit or prevent access to the device modules, applied access control protocol, disable any built-in applications, enable or restrict cloud and disk backups, and/or impose the device authentication rules).

If a device is unable to prove algorithmically that it is viable as a legitimate node, it will be denied access to the IIoT network until such time as it can authenticate itself. Until then, it will be denied access. In this context, overcrowding and interference to OSI (open systems interconnection) layers, such as the ‘physical layer’ in an IoT industrial context will hinder sensors from finding threats such as fire, overflow, and unexpected movement.

Step 4: Quarantine of unsecured devices

Nodes positioned in a specific cluster were deferred from endorsing wireless networks when a security risk is identified on one of IoT nodes. In this hypothetical situation, the cooperating node was isolated while neighbor-linked devices were permitted to join the wireless network. To make this method essentially relevant, each periodic interval or unfriendly encounter will generate an alert notification that is essential to consistently evaluate the threat of risk broadcast from the Zigbee gateway.

The seven-step process by which the transaction server defines the access status of an interconnected IIoT device was developed. The following conditions must be met for the configured server to obtain the desired results:

(a) Is the node legitimate?
(b) Is the Sync protocol [20] feature enabled? If a device is not synchronized, it will not be able to join the network, regardless of whether or not it is compatible with certain IoT nodes.
(c) Is the device subject to a particular exception which blocks the device, such as operability and packet exchange capability?
(d) Does the device have a particular exception that allows the device?
(e) Is the device scrambled by an appropriate node access rule?
(f) Is the device restricted by an access rule for the corresponding node?
(g) Does the device have a corresponding node access rule?

Using a data variable model "A", the node quarantine process constructs a set of segregations (s-Set), "C", using the following steps:

(1) Indiscriminately choose a characteristic 'b' and a riven assessment ratio 'm'.
(2) Split 'A' into two subclasses by exhausting the rule b < m. The subgroups will match to a left and right sub-tree in 'C'.
(3) Repeat both steps 1 and 2 recursively, as long as the selected node has only one template or all results in the current node share the same values.

The procedure then repeats steps 1, 2 and 3 repeatedly to generate the required segregation package. According to the aforementioned criteria (a–g), the isolation set and characteristics of incoherent points were formed. By analyzing the outcome data, it was concluded that most irregular points will be situated nearby to the source of the established node modeling tree, since they are easier to quarantine when equated to normal node behavior and program signature points.

Once we have a group of Quarantine node sets, the procedure exploits the succeeding variance score, assuming a data point '*d*' and a segmentation size of '*f*':

$$r(d,f) = 2^{\frac{-J(k(d))}{n(f)}} \tag{5}$$

Here $k(d)$ signifies the distance between the data point 'd' in a specified Quarantine node set. The manifestation '$J(k(d))$' indicates the probable or "regular" assessment through all the Segregation node sets. The indicator '$n(f)$' characterizes the typical significance of '$k(d)$' assumed a model size of 'f' and is demarcated by means of the resulting equation.

$$n(p) = \begin{cases} 2K(p-1) - \frac{2(p-1)}{z} \; for \; `f > 2' \\ 1 \; for \; `f = 2' \\ 0 \; otherwise \end{cases} \tag{6}$$

Once the irregularity ratio '$r(d,f)$' is calculated for a specified criterion, it is possible to perceive inconsistencies by means of the succeeding benchmarks:

(1) If $r(d,f)$ is close to 1 then '*d*' is probable to be an inconsistency.
(2) If $r(d,f)$ is less than 0.5, then '*d*' is assumed to be a valid node.
(3) If $r(d,f)$ is adjacent to 0.5 for all of the criteria in the adopted ruleset and dataset, then the analysis does not indicate any anomalies.

Step 5: Policy lifecycle management

The policy-based management approach offers a clever solution to the issue of managing complex systems. It provides a process for rationalizing and primarily systematizing the device management protocol. To perform the described functions, a policy lifecycle model was programmed based on recognized software development techniques that control the use of a policy-based data management system within an IIoT.

In Figure 2, the flow represents the 'key steps and related actions' according to the policy lifecycle. The data stream exhibits the activity's results and responses. The reverse path indicates the probable reverse engineering in terms of the life cycle of the procedure, the identification of events, the evaluation of events, the definition of policy, the applicability of policy and, finally, the erasure of policies. It is worth highlighting that consistent communication faces a significant obstacle in the form of the need to set up sufficient security for accessible systems. Thus, the safety of integration networks is a major concern, alongside their accessibility.

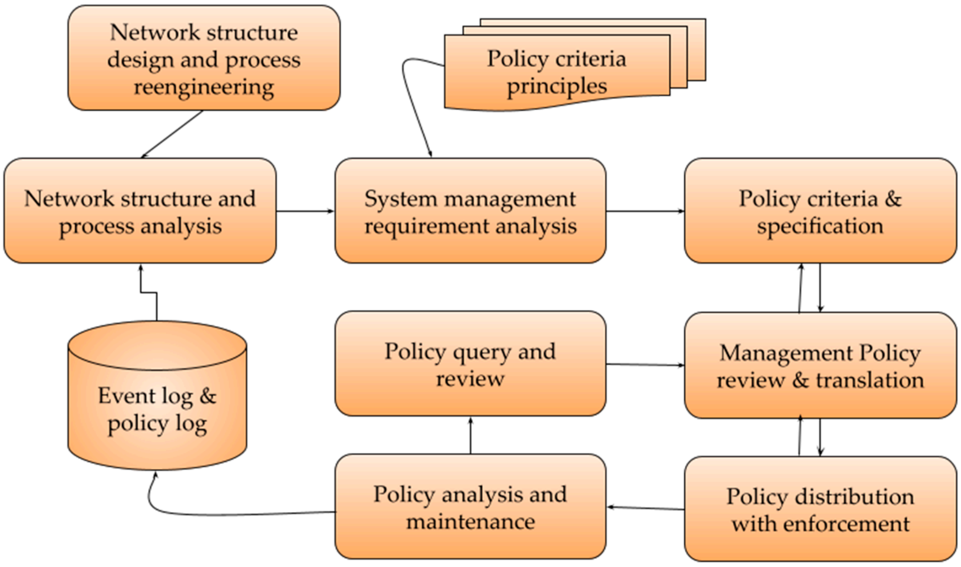

Network structure design and process reengineering
Policy criteria principles
Network structure and process analysis
System management requirement analysis
Policy criteria & specification
Event log & policy log
Policy query and review
Management Policy review & translation
Policy analysis and maintenance
Policy distribution with enforcement

Figure 2. Policy lifecycle management.

Step 6: Overall security posture assessment

As the IIoT network extends, it is beneficial to perform regular security assessments of the platforms, equipment, nodes and IoT protocols that are being used. In general, there are few security procedures that are relevant to the purposed asset classification, such as: (a) keep the device firmware up to date; (b) auditing of nodes in real-time and historical activity log; (c) filter message/transmission brokers; and (d) backup CMDB database.

The proposed scheme exploits the 'Bayes estimator' filter [21] to access the overall security posture, which is vital to obtain computational efficiency (i.e., time and memory required to accomplish the required task). To measure the errors, the author used the meta-analysis where the aggregated implications from many data tables are brought together to make the interpretation. The Bayes framework is primarily suitable for meta-analysis, as each prior experimental outcome can be retained as providing a glaring dimension of an essential measure of interest. Following that, the prototype monitors directly from two modules: (a) a precedent on the core capabilities and (b) a capacity-error-style prototypical for each of the datasets examined.

Considering Figure 3, it was evident during experiments that the Bayes estimators failed to perform while deployed in the high multimodality scenarios, as there is no way to evaluate all integrals involved in the subsequent projection inference.

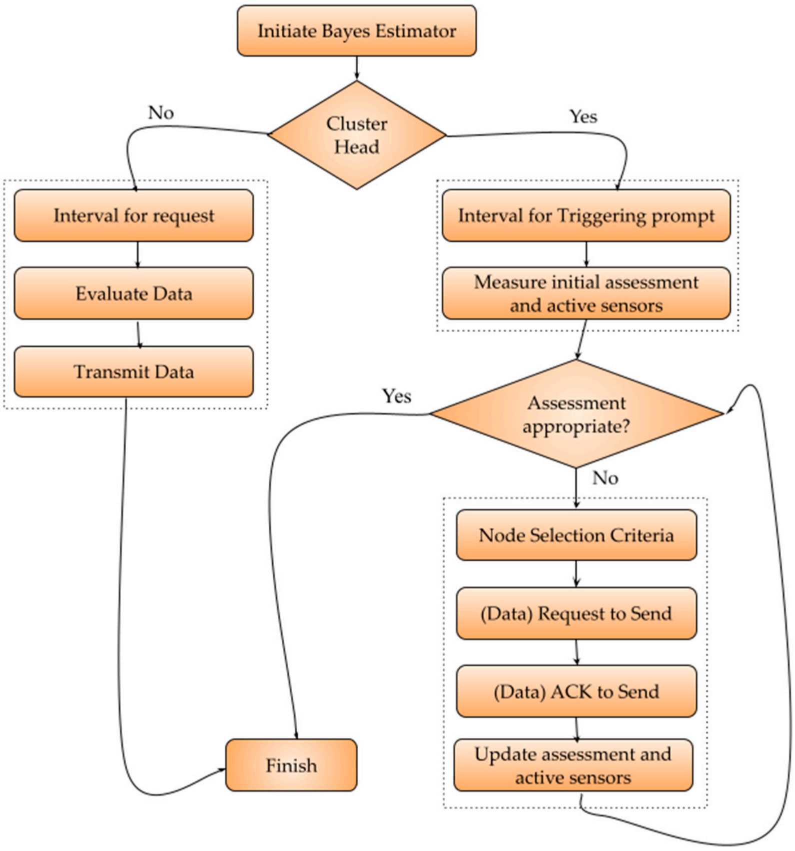


Figure 3. Flow diagram for data retrieval and evaluation from sensing nodes.

Mean 'μ_u' and variance 'σ_u' of the marginal distribution of $d_1, d_2, \ldots, d_m$ using maximum likelihood technique:

$$\widehat{\mu_u} = \frac{1}{m}\sum d_y,\ \widehat{\sigma_u^2 = \frac{1}{m}}\sum \left(d_y - \widehat{\mu_u}\right)^2 \tag{7}$$

Once data is computed, the 'law of total expectation' and 'law of total variance' was applied to evaluate μ_u and σ_u^2:

$$\mu_u = P_\pi[\mu o(\theta)],\ \sigma_u^2 = P_\pi[\sigma_o^2(\theta)] + P_\pi[(\mu o(\theta) - \mu_u)^2], \tag{8}$$

where $\mu o(\theta)$ and $\mu o(\theta)$ are instances of conditional distribution $o(d_y|\theta_y)$ that is a known variable. Once the iteration is complete, system assumes that $\mu o(\theta) = \theta$ and that $\sigma_o^2(\theta) = W$, thus

$$\mu_\pi = \mu_u,\ \sigma_\pi^2 = \sigma_u^2 - \sigma_o^2 = \sigma_u^2 - W \tag{9}$$

Finally, framework aggregates the estimated event analysis data,

$$\widehat{\mu_\pi} = \widehat{\mu_u},\ \widehat{\sigma_\pi^2} = \sigma_u^2 - W \tag{10}$$

Step 7: Automated incident response through policy enforcement

Incident response is a set of fixed rules that the enterprise (IIoT infrastructure) practices to detect, understand and root out cyber-attacks. The purpose of the incident response is to quickly identify and stop the attacks, reduce the anomaly and thwart future attacks of the corresponding type. Throughout the identification, all data collected was secured (using the Keccak-512 hash [22]) and reserved for semi-automated deep mining. Once an anomaly was observed, victim devices were contained for a short interval (i.e., until the automated process fixes the adversary-driven malfunction, as per the predefined registry (i.e., event, alert, and incident)). Anticipated outcomes include: (a) anomaly detection and analysis, (b) threat exclusion, and (c) remediation. Best practices were applied based on (but not limited to) the following:

(a) Industrial IoT nodes have been pre-arranged in various clusters based on node features such as location and material type.
(b) Industrial IoT nodes could be searched by active functions, such as connectivity rank, software type, application eminence and node status.
(c) Installation (device and software) rollouts were actively monitored and were automatically halted if IoT nodes fail to sustain the pre-defined performance indicators (such as: device and application response time in milliseconds, TCP (Transmission Control Protocol) uplink/downlink, communication round trip time, packet loss (percentage) for uplink and downlink, error rate, and yield throughput).
(d) Resilience ratio of errors during firmware updates.
(e) Automatic logging of contextual information related to device activity.
(f) Quarantine the error-prone device which, after identification, will be autonomically fixed (i.e., in accordance with firmware requirements).

Table 4 presents the results as the applied layers are stand-alone and the associated functionality is achieved through various means. Consequently, if an intruder disrupts the system, the anomaly still outshines many security obstacles with dissimilar strengths and flaws before accomplishing its mission.

Table 4. Goals achieved by the proposed security steps. (no ×), (yes ✓), (some-circumstances ○).

To Network and Devices	Physical Layer	Sensing Edge/Boundary	Internal Network	Host	Applied Application	Information
Controlling physical admittance	✓	○	○	○	○	×
Restricting logical access	×	✓	✓	○	○	○
Reinforcement	✓	○	✓	✓	○	○
Defending undesirable alteration of data	✓	○	○	✓	✓	✓
Observing applied protocols	×	✓	✓	✓	✓	×

Policy management, as conceived by the author, is the process through which a given infrastructure's policies and protocols are created, implemented, maintained, and managed. Policy management enforces the applicable system effectively to evaluate the effects of data catalogue, system architecture and modeling, data-driven operations, data and process sharing and value realization. Control configuration permits proposed the scheme to administer the device profiling, manage authentication, apply security posture assessment, and enforce automated incident response through policy enforcement.

5. Performance Evaluation

The assessment of the proposed scheme is carried out in three parts. In the first part, an enterprise-specific case study is reflected to evaluate various processes of the zero-tolerance security system. In the second part, the implementation of the proposed scheme relies on many factors such as payload, expected output, and false positives. In the 3rd part, the suggested security model is assessed.

Experiments were conducted on-site of the interlinked 'IIoT' which were being operateable remotely based on data aggregation, processing and analyzation (mainly a threat to base station). The functional testbed was equipped with plug and play wireless sensors. IoT sensors have been installed and programmed to guarantee high data reliability and accuracy, with the privilege of modifying the network topology in accordance with the requirements. Details of assessment setting are illustrated in Table 5.

Table 5. Evaluation Environment.

Product	Specification
×86 Computers	Long-lasting industrial standardized computing equipment.
ZigBee Router (RM-23BZBSR)	Transmits supervision signal for application to augment routing consistency.
Magnum 10RX Router	16× GbE, 10× WAN, 32× Serial
Operating System	Moxa Industrial Linux
Enterprise data Storage	PowerVault ME4012 (2.2 GHz, 2-core) with maximum capacity of 3 PB
Network Type	Heterogeneous
Surveillance Type	SCADA
Sensors	NCD IoT Cycle Counter Transmitters, Pressure Sensor Transmitters, Activity Sensor Transmitters
Packet Analyzer	Wireshark
Connection-oriented protocol	TCP
Data Acquisition Protocol	MQTT (Message Queuing Telemetry Transport)
Data Broadcast Protocol	DDS (Data Distribution Service)
Average Packet Length	1500 bytes
Data Outcome Format	PCAP file
Total Number of Samples	200,000 samples
Evaluated Attack Types	Remote Code Execution. Nmap Scanning, Command Injection, Man-in-the-middle attack (MITM), DoS (denial of service), Malicious Latency Protocol, Legacy Protocols, and Cryptojacking.

A thorough scan of all likely attacks was not feasible. In this article, we focus on an explicit attack scenario which demonstrates the utility of the simulated system environment. We evaluated for five hours to understand the behavior of multiple device behaviors in different scenarios.

The functionality of the data driven system is largely dependent on the methods used for encryption. On the other hand, such methods use up a considerable amount of computational resources, such as time on the central processing unit (CPU), memory, and even battery power. Many IoT devices, particularly those that are installed at the edge of the network, have limited battery capabilities. Several attacks try to deplete edge nodes' resources and batteries. Figure 4 illustrates the battery consumption outcome of wireless and mobility-driven IoT devices for scenarios such as node advertisement, scanning and handshake. In this context, the baseline was marked as a mode in which the node is in a state of inactivity and there is a minimal overhead for communication. Awareness of battery status information is critical to understanding process energy efficiency and to reveal any ongoing node-related cyber-attacks, such as searching for gaps in accelerometer measurements.

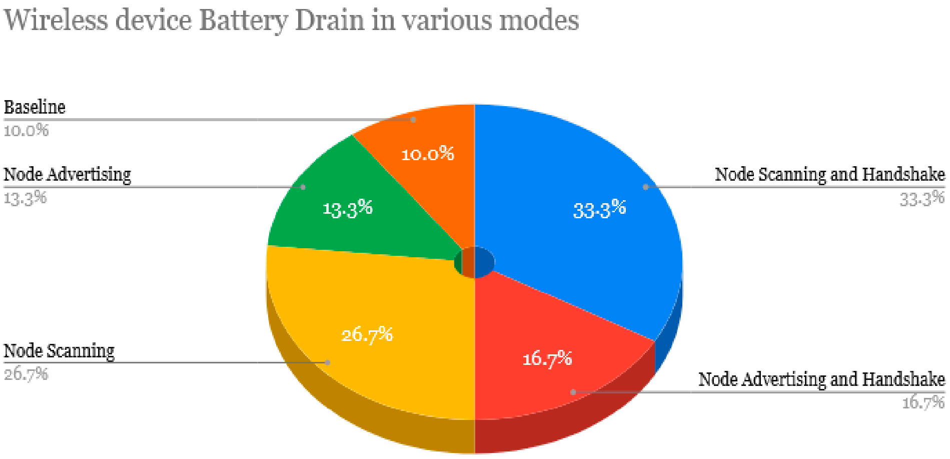
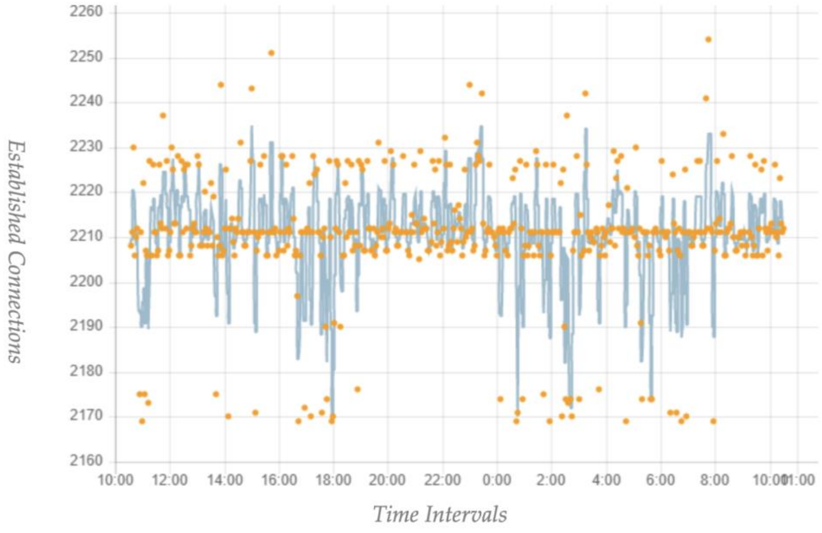


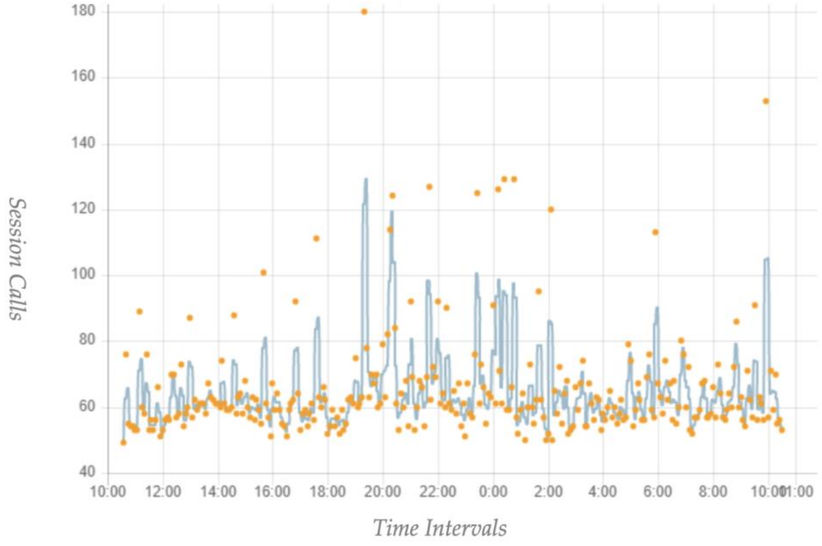
Figure 4. Power consumption in cryptographically aware modes.

In Figure 5a–f, node status and the value 'number of connections' for device-to-device paradigm was used to evaluate probability estimation function to examine transmission power among devices. This is an important factor in determining the radius range of the cell, which is particularly useful for IEEE 802.15.4 compatible networks. For network level threshold evaluation (i.e., Data-path and Control-path CPU, memory, and total number of tunnels and devices), the brute force investigation was conducted. Based on assessment outcome, the author also envisioned the following roles for vulnerability assessments:

(a) Examining assets for potential security flaws.
(b) Ranking the severity of the risks associated with these vulnerabilities.
(c) Fixing security flaws through applying patches, managing configurations, or setting up workarounds.

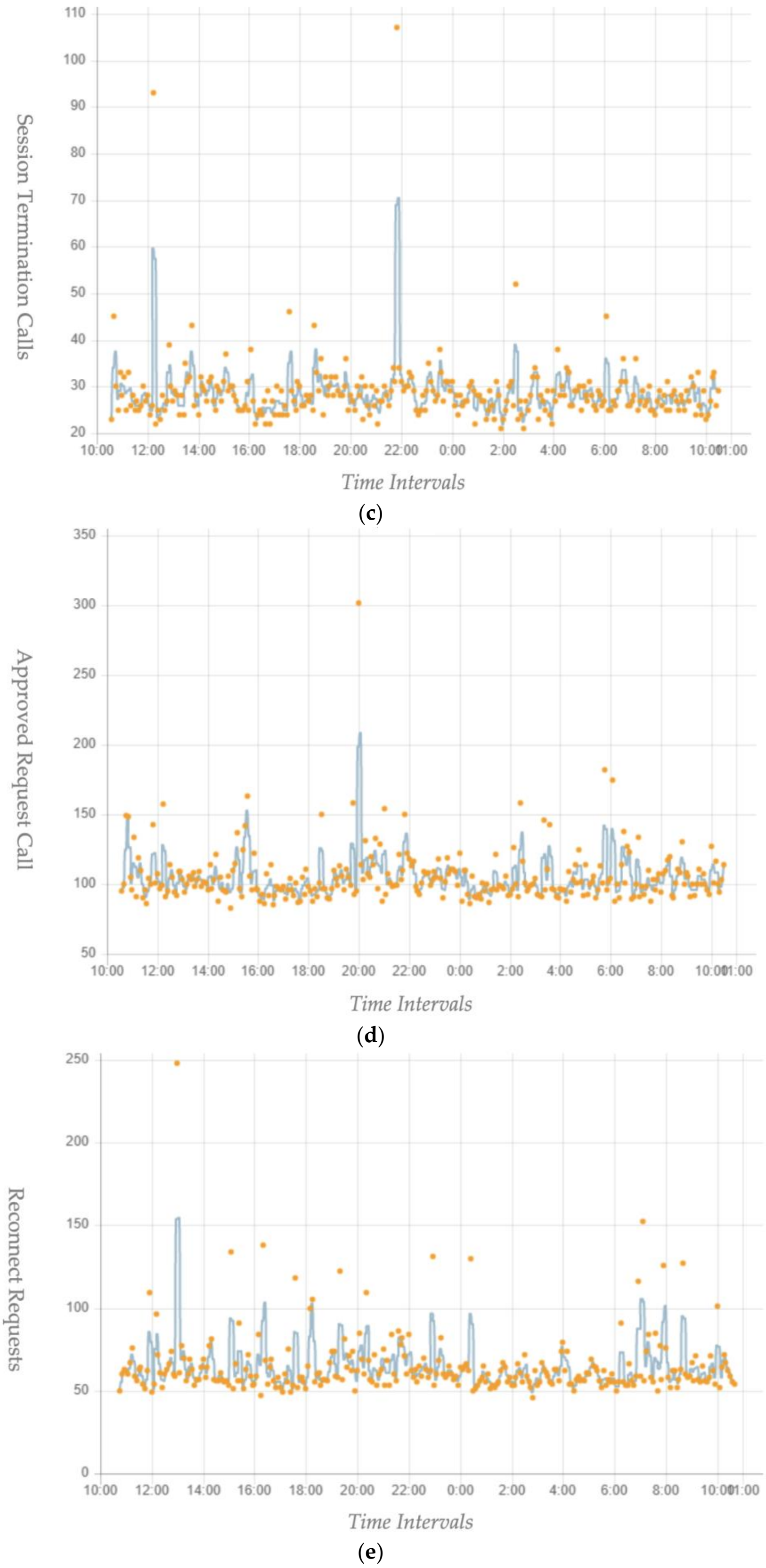


(**a**)



(**b**)

Figure 5. *Cont.*

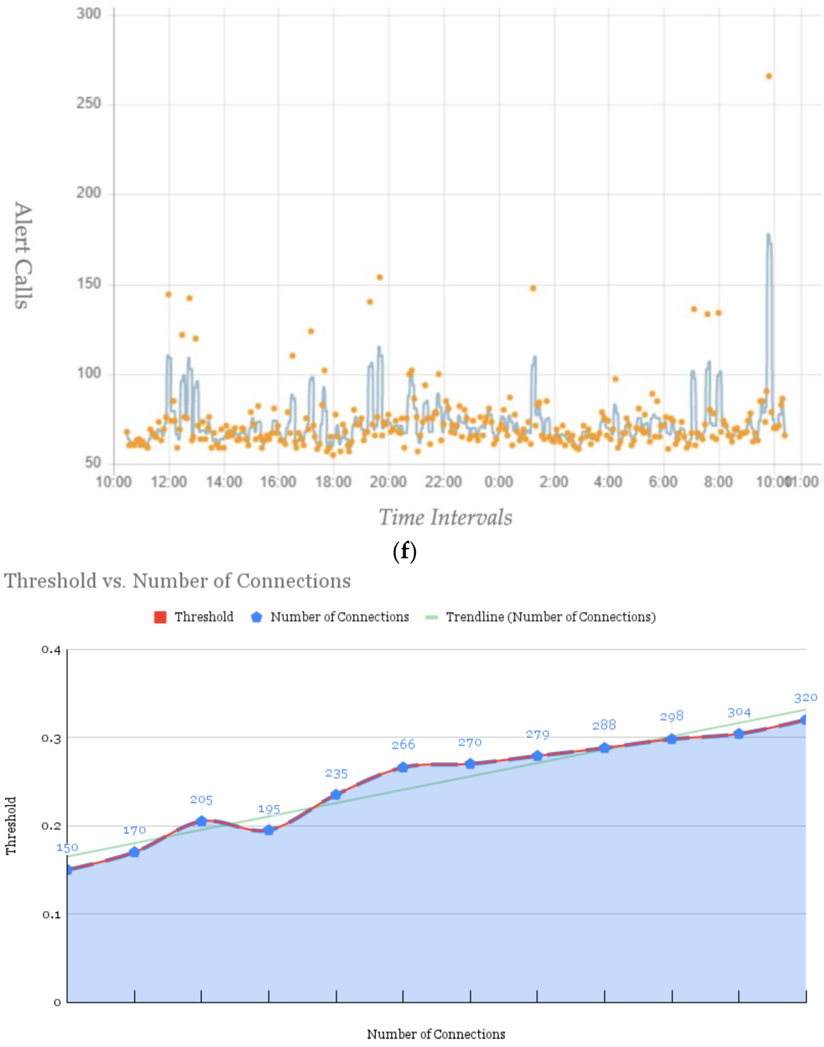


(**c**)

(**d**)

(**e**)

Figure 5. *Cont*.



(**f**)

(**g**)

Figure 5. Network Status. (**a**) Server Connections. (**b**) Established Node Sessions. (**c**) Session Disconnections. (**d**) Sessions Deleted. (**e**) Session Reconnect Data. (**f**) Alert Generated Data. (**g**) Threshold vs. Number of Connections.

Figure 5g illustrates that when a threshold variable exceeds the predefined percentage/value depending on the policy, an action alert is issued. In the projected scheme, three states were defined: (a) Normal (value between 0 to 25 percent), (b) Minor (value between 26 to 55 percent), and (c) Major (value greater than 56 percent). The optimal threshold range was determined by analyzing the recorded "trace file" for control point nodes. Warning alerts were related to access denial (such as failed read), unauthorized FTP (file transfer protocol) connections, process-killed, device shutdown, unauthorized connection, usage of special privilege, fail to use authorized privilege and system reboot.

While it was essential to conduct a certain level of vulnerability assessment, management framework combined this with the discovery process into a single stage. Ultimately, projected framework was able to complete the loop and speed up fixes for vulnerabilities to lessen risk. The zero trust loop consisting of the analysis for data, devices, applications, and network traffic.

The scheme used asynchronous and acyclic data transmission mode to send data bits at any point in time because: (a) IoT devices may communicate at irregular intervals, (b) data transmission accuracy requirement is high, and (c) is applicable for short-distance data transfer. As per Figure 6, the scheme evaluated the performance of the system when the 'y' axis is exhibited in units of packets/second. Each IoT device was connected point-to-point bidirectional, which is a positive scenario for ad hoc network topology. The communication properties of the acyclic data transmission were aligned with the data value status (burst transfer, timeout, MN space), event alerts (interruptions, processing requests, data transfers) and device data.

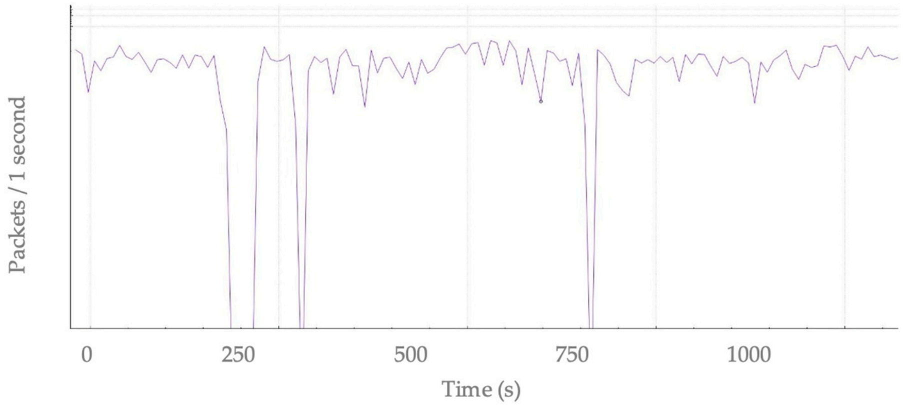
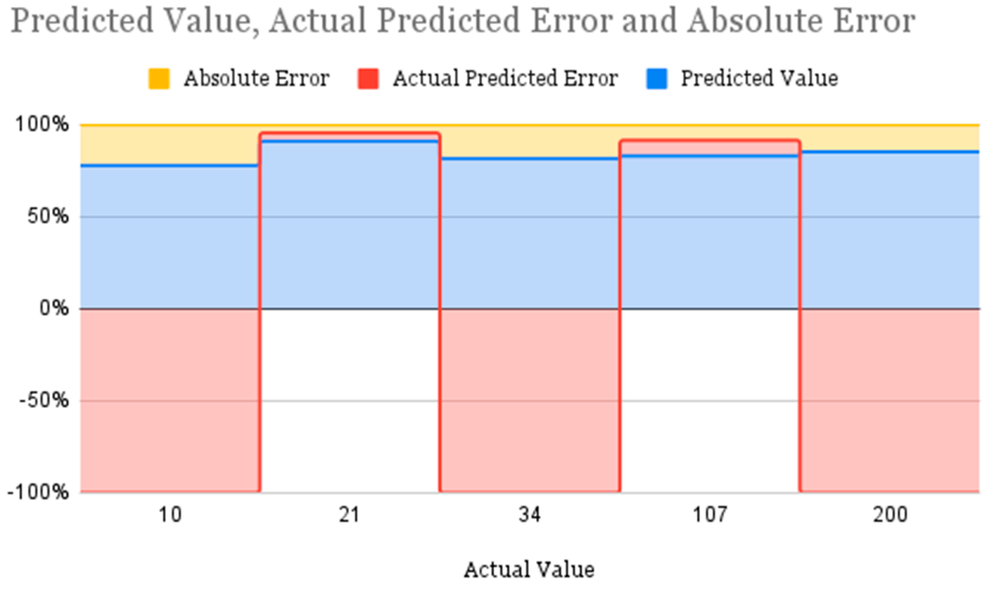


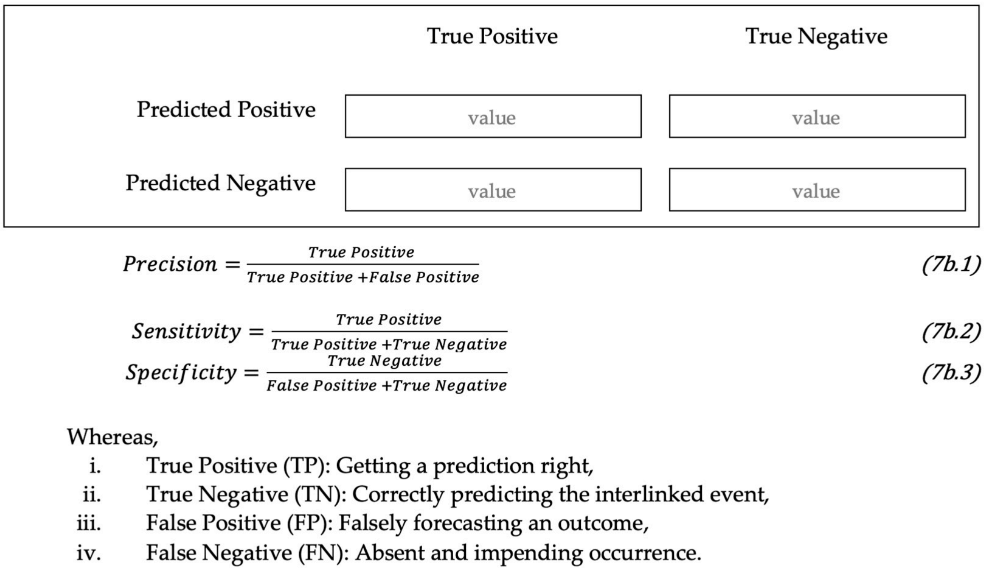
Figure 6. Device level Wireshark I/O graph (1000-s dataset) for normal data transmission environment.

As an evaluation metrics for classification problems where the output might be multi-class classifiers, the Confusion Matrix is incredibly helpful for assessing Recall, Precision, Specificity, and Accuracy. To validate and improve the efficiency of the scheme, the sensitivity of the anomaly sensor (true positive), true negative (specificity), false positive and false negative (anomaly rate) was periodically assessed (Figure 7). The true positive represents the probability of an accurate fault detection, while the true negative represents the probability of a negative test, as the device is legitimate and correctly functional. The sensitivity and specificity threshold has been programmed to be modified depending on target infrastructure precision requirements.



(**a**)

Figure 7. *Cont*.



	True Positive	True Negative
Predicted Positive	value	value
Predicted Negative	value	value

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \tag{7b.1}$$

$$Sensitivity = \frac{True\ Positive}{True\ Positive + True\ Negative} \tag{7b.2}$$

$$Specificity = \frac{True\ Negative}{False\ Positive + True\ Negative} \tag{7b.3}$$

Whereas,

i. True Positive (TP): Getting a prediction right,
ii. True Negative (TN): Correctly predicting the interlinked event,
iii. False Positive (FP): Falsely forecasting an outcome,
iv. False Negative (FN): Absent and impending occurrence.

(**b**)

Figure 7. Confusion Matrix Chart with information generated and fetched from five initial datasets. (**a**) Confusion Matrix Outcome. (**b**) Automated data-driven Confusion Matrix Calculator.

Table 6 provides a comparative analysis of schemes that were discussed and evaluated in contrast with the proposed scheme with respect to solution time, used method, and demonstrated outcome and research gaps.

Table 6. Comparative Analysis.

	Solution Type	Method Used	Consequences Claimed	Research Gap
Nakamura et al. [23]	Risk Assessment (accidental, malicious, natural)	Confidentiality, resilience, influence assessment and trustworthiness representing incidents in IIoT	Comparatively efficient	Administration and execution enrichment is compulsory
Wu et al. [24]	Enhancement in SCF-MCLPEKS scheme	Searchable public key encryption	Latency free retrieval of encrypted data	Inadequate to device level security
Ma et al. [25]	SCF-MCLPEKS	Bilinear Pairing	Diminished process computation time, and communication cost	Application focused and limited to anomaly type
Amin et al. [1]	SAMIIT: adversarial tactics, techniques, and common knowledge	Machine learning focused anomaly classified IDS	Mapping alerts to attack segments	Improvement for real-time application with inadequate to device level security
Bassam et al. [2]	Risk assessment system, clustering technique	Intrusion detection system	Discovered several risks caused by the IT/OT (information technology (IT) systems with operational technology (OT) systems) union	Processing delay with extraordinary computational cost
Hussain et al. [3]	Multi-Layer security	FPGA and PUF-based system security	Satisfactory security framework with high computational capabilities and flexible architectures	Behavior configurations can be considered to make proposed scheme less exposed to anomalies
Kumari et al. [4]	QoS aware secure Peer-to-Peer network	Blockchain-based protected distributed model	Enhanced data load balancing with reduced communication delay	Processing delay, application centric protocol security gaps should be addressed (i.e., accuracy, detection, mitigation, etc.)
Proposed Scheme	Detection and Moderation	Automated authentication, profiling. DoS for malicious node, and policy management	Secured network transmission, reduced computational cost, diminished energy consumption	Performance augmentation is vital

In reference to Tables 3 and 6, Figure 8 highlights the comparative assessment of the proposed methodology aligned with previously published research. It is evident that there are no solutions that can meet all the needs that have been outlined. Nevertheless, the proposed strategy has the potential to greatly enhance the IIoT system's security and reliability while also decreasing communication congestion.

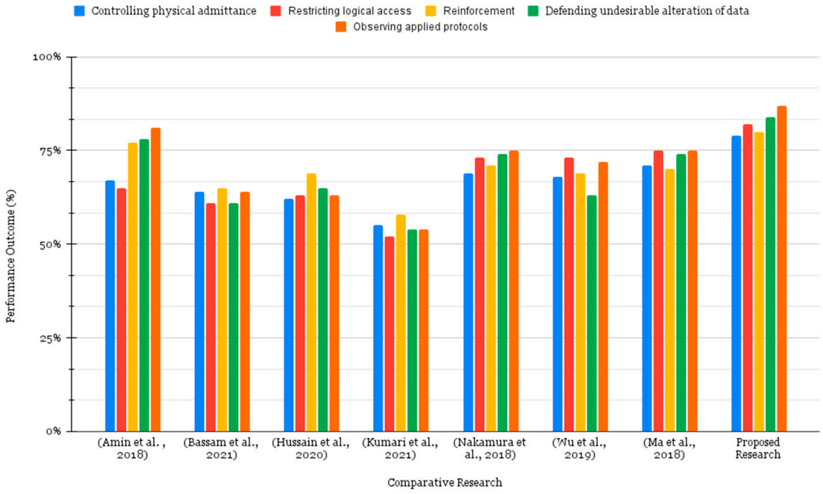


Figure 8. Comparative analysis.

To understand normal and abnormal activity, the proposed method closely monitors energy consumption routines of manually selected IoT devices. Putting power optimization at the forefront of experimental implementation was essential for achieving optimal device performance. Energy consumption was observed during different device modes, such as 'no sleep/active', 'light sleep' and 'deep sleep'. In active mode, the IoT node never sleeps and hence constantly uses energy. The device's CPU and internal clock are put to light sleep when the node is idle for a while. The device's real-time clock remains powered throughout deep sleep. Deep sleep saves the greatest energy. This even works effectively for IoT nodes that provide data before sleeping. Figure 9 reflects that IoT nodes periodically transmit data packets and of 'status variations, environmental variabilities, access or usage attempts, and anomalous states'. It was observed that the transmitters inside of IoT devices have a higher power need than the modules' processors and memories. By understanding the energy consumption log data in the legitimate and anomaly-driven environment state, the proposed method used energy consumption irregularities as an indicator of malware risk that will trigger the framework to initiate deep evaluation and will re-authenticate via device profiling.

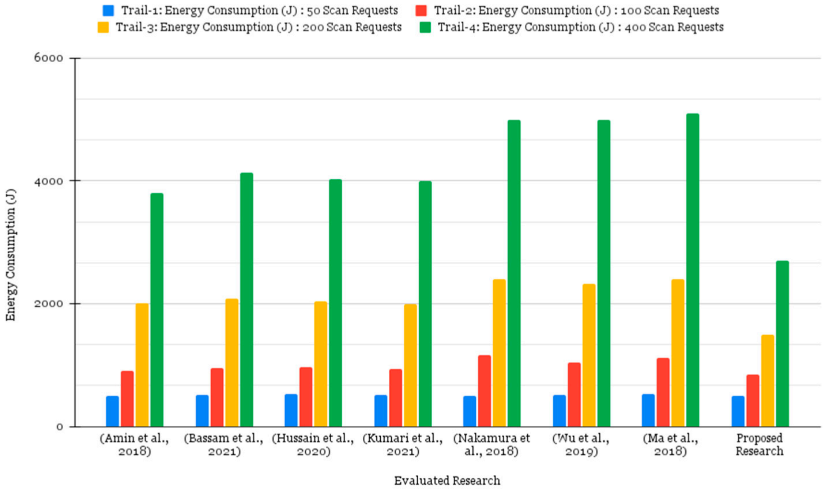


Figure 9. Energy analysis.

There is a need for minimal lag time between sending a request and receiving a response in a low-latency Internet of Things device. To fully realize the promise of the Internet of Things, academics are always focusing on ways to decrease the reaction time. Thus, a high-capacity, low-latency network is required to enable ultrafast data transmission and processing, which is essential for IIoT devices and applications to function in real-time. Figure 10 illustrates the variable latency time for events of varying sizes (bytes). On average the data packet size was 1500 bytes. Analyzed methods observed latency due to data management bottlenecks, device update delays, infrequent connections, ad hoc network topology, and repetitive node profiling and authentication. The proposed scheme has used latency data to:

(a) locate underutilized resources and connections.
(b) reduce the complexity of prioritizing devices and connecting them.
(c) better data management by transferring useful data to the network's periphery.
(d) improve the efficiency of a network system.
(e) introduce new application potential,

Device-Oriented Commendations

(a) Periodically, verify the 'clock-sync' to sustain serial communication paradigm.
(b) All data stored and transmitted from devices must be encrypted to achieve the privacy requirement.
(c) Remote execution of privileged instruction (i.e., read and write control registers which varies in Bit count from 8 bits to 16 bits) should verify the source credentials.
(d) The eligible device must be capable of scanning the desired TCP port for device characteristics.

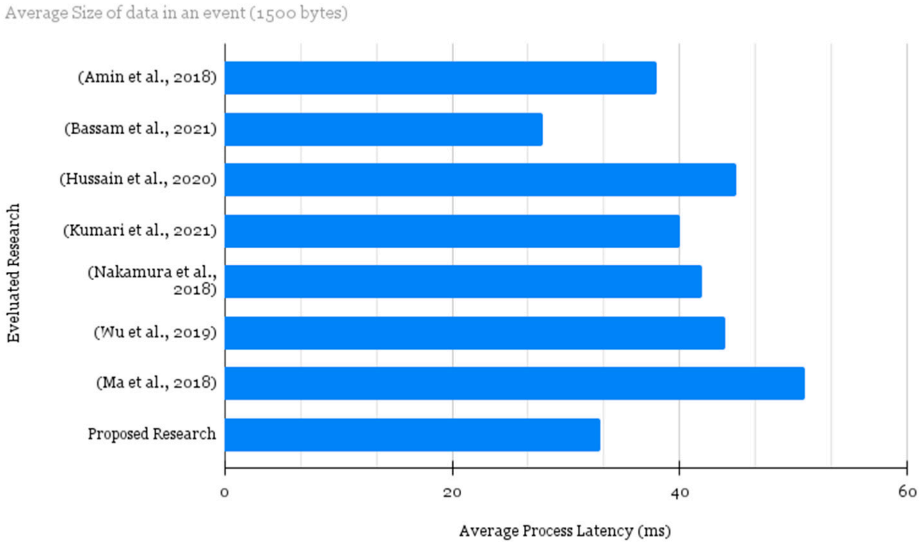


Figure 10. Variable latency time for events of varying sizes (KB).

6. Conclusions

To encounter industrial requirements, a scalable and secure data driven infrastructure is a necessity. Large-scale computing requires disruptive technologies to protect IIoT infrastructure while interacting swiftly with risk assessment and prevention modules. In this paper, a zero trust confidential computing paradigm was programmed in JavaScript to (a) accurately consolidate data, (b) furnish efficient network access to IoT nodes, processes, and applications. To validate the proof of concept, estimates were made at an IoT-compatible "indoor facility", which relies heavily on a consistent flow of reliable data flows to meet functional requirements. The result of the evaluation was satisfactory, which led to an efficient and secure IoT ecosystem. By effectively applying the Zero Trust Model, the framework was able to:

(a) Protect communication no matter where the interconnected node is located,
(b) Allow admission to distinct resources only on a per-session basis,
(c) Manage the input of nodes to resources through a set of active rules,
(d) Evaluate the security rating of all assets while assessing requests,
(e) Sustain an uninterrupted cycle of permitting/rejecting access, scanning and weighing risks, adjusting, and constantly re-valuing trust in enduring communications, and
(f) Accumulate information related to data and interconnected devices to autonomously improve network behavior.

Future Work

Stakeholders can be at risk when it comes to making technological decisions based on the current state of the zero trust paradigm. Each provider has their own unique take on the subject, and not all products are created equal. Based on this study, the following potential contributions can be made in the future:

(a) It is possible to investigate implementing Blockchain on the FPGA hardware itself.
(b) The proposed approach is capable of being evaluated in relation to a variety of various cyberattacks.
(c) Further optimization of the proposed system is possible by establishing limits for data exploration, monitoring, and discovery.

Funding: The author would like to acknowledge the support of the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project 2021/01/17623.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares that he has no conflict of interest to report regarding the present study.

References

1. Amin, H.; Burkett, R. SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases. In Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research, Hamburg, Germany, 29–30 August 2018; pp. 11–20.
2. Bassam, Z.; Hussaini, A.; Ali-Gombe, A. IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, 26–28 April 2021; pp. 305–307.
3. Hussain, A.; Johnson, A.; Hill, R.; Lane, P.; Alsboui, T. Hardware-intrinsic multi-layer security: A new frontier for 5G ena-bled IIoT. *Sensors* **2020**, *20*, 1963.
4. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain-Based Massive Data Dissemination Handling in IIoT Environ-ment. *IEEE Netw.* **2021**, *35*, 318–325. [CrossRef]
5. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [CrossRef]
6. Rahman, M.; Jahankhani, H. Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-attacks. In *Information Security Technologies for Controlling Pandemics*; Springer: Cham, Switzerland, 2021; pp. 307–334.
7. Du, R.; Zhen, L. Multiuser physical layer security mechanism in the wireless communication system of the IIOT. *Comput. Secur.* **2022**, *113*, 102559. [CrossRef]
8. Goswami, P.; Mukherjee, A.; Maiti, M.; Tyagi, S.S.K.; Yang, L. A neural network based optimal resource allocation method for secure IIoT network. *IEEE Internet Things J.* **2021**, *9*, 2538–2544. [CrossRef]
9. Xiong, H.; Wu, Y.; Jin, C.; Kumari, S. Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT. *IEEE Internet Things J.* **2020**, *7*, 11713–11724. [CrossRef]
10. Li, J.; Lyu, L.; Liu, X.; Zhang, X.; Lv, X. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4059–4068. [CrossRef]
11. Nguyen, T.A.; Min, D.; Choi, E.; Lee, J.W. Dependability and security quantification of an internet of medical things infrastructure based on cloud-fog-edge continuum for healthcare monitoring using hierarchical models. *IEEE Internet Things J.* **2021**, *8*, 15704–15748. [CrossRef]

12. Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity model based on hardening for secure internet of things implementation. *Appl. Sci.* **2021**, *11*, 3260. [CrossRef]
13. Kim, H.Y.; Xu, L.; Shi, W.; Suh, T. A secure and flexible FPGA-based blockchain system for the IIoT. *Computer* **2021**, *54*, 50–59. [CrossRef]
14. Taheri, R.; Shojafar, M.; Alazab, M.; Tafazolli, R. Fed-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT. *IEEE Trans. Ind. Inf.* **2021**, *17*, 8442–8452. [CrossRef]
15. Chia-Shin, Y.; Chen, S.; Li, I. Implementation of MQTT protocol based network architecture for smart factory. *Proc. Inst. Mech. Eng. Part B J. Eng. Manuf.* **2019**, *235*, 2132–2142.
16. Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [online] Request for Comments: 5280. Available online: https://datatracker.ietf.org/doc/html/rfc5280 (accessed on 24 April 2022).
17. Tariq, U.; Aseeri, A.O.; Alkatheiri, M.S.; Zhuang, Y. Context-Aware Autonomous Security Assertion for Industrial IoT. *IEEE Access* **2020**, *8*, 191785–191794. [CrossRef]
18. Buddhadeb, P.; Vijayakumar, V.; Pratihar, S.; Kumar, D.; Reddy, K.H.K.; Roy, D.S. A genetic algorithm based energy efficient group paging approach for IoT over 5G. *J. Syst. Archit.* **2021**, *113*, 1–8.
19. Dimitrios-Georgios, A.; Harishankar, M.; Weber, M.; Tague, P. Zigator: Analyzing the security of zigbee-enabled smart homes. In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 8 July 2020; pp. 77–88.
20. Xuxin, Z.; Liu, Y.; Zhang, Y. A Secure Clock Synchronization Scheme for Wireless Sensor Networks Against Malicious Attacks. *J. Syst. Sci. Complex.* **2021**, *33*, 1–14.
21. Jinxin, L.; Kantarci, B.; Adams, C. Machine learning-driven intrusion detection for contiki-NG-based IoT networks exposed to NSL-KDD dataset. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, New York, NY, USA, 16 July 2020; pp. 25–30.
22. El, M.S.; Fettach, M.; Tragha, A. High frequency implementation of cryptographic hash function Keccak-512 on FPGA devices. *Int. J. Inf. Comput. Secur.* **2018**, *10*, 361–373.
23. Nakamura, E.T.; Ribeiro, S.L. A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems. In Proceedings of the Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4 June 2018; pp. 1–6.
24. Wu, T.Y.; Chen, C.M.; Wang, K.H.; Wu JM, T. Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments. *IEEE Access* **2019**, *7*, 49232–49239. [CrossRef]
25. Ma, M.; He, D.; Kumar, N.; Choo, K.-K.R.; Chen, J. Certificateless searchable public key encryption scheme for industrial Internet of Things. *IEEE Trans. Ind. Inf.* **2018**, *14*, 759–767. [CrossRef]