Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Decentralizing Trust in Boundary Attack Analysis: A Blockchain-Enhanced Complex Network Modeling Framework for Power IoT

Xin Li

submission_qpzm@163.com

Northeast Electric Power University

Zhaoyang Qu

Northeast Electric Power University

Tong Yu

People's Bank of China

Ming Xie

China Southern Power Grid Guangxi Power Grid Co., Ltd.

Fu Yu

China Southern Power Grid Guangxi Power Grid Co., Ltd.

Wei Ding

Qilu University of Technology (Shandong Academy of Sciences

Research Article

Keywords: Power IoT, Blockchain, Boundary Attacks, Complex Networks, Risk Modeling, Traceability

Posted Date: May 14th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9220624/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Decentralizing Trust in Boundary Attack Analysis: A Blockchain-Enhanced Network Modeling Framework for Power IoT

Xin Li[1*], Zhaoyang Qu[1*], Tong Yu[2], Ming Xie[3], Fu Yu[4], Wei Ding[5,6]

[1*]School of Electrical Engineering, Northeast Electric Power University, Street, City, 100190, Jilin, China.
[2]Qinghai Provincial Branch, People's Bank of China, Street, Xining, 810000, Qinghai, China.
[3]Research Institute, China Southern Power Grid Guangxi Power Grid Co., Ltd., Street, Nanning, 530023, Guangxi, China.
[4]Bijie Power Supply Bureau, China Southern Power Grid Guangxi Power Grid Co., Ltd., Street, Bijie, 551700, , China.
[5]Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Street, Jinan, 250014, Shandong, China.
[6]Shandong Provincial Key Laboratory of Computer Networks, Shandong Fundamental Research Center for Computer Science, Street, Jinan, 250014, Shandong, China.

*Corresponding author(s). E-mail(s): submission_qpzm@163.com;

Abstract

Power Internet of Things (Power IoT) systems are increasingly exposed to sophisticated boundary attacks due to their high connectivity and heterogeneous network structures. Traditional web-centric analysis methods primarily focus on static topology or localized interactions, lacking effective mechanisms for global attack propagation modeling and trustworthy traceability. To address these challenges, this paper proposes a complex network-based framework for modeling and analyzing boundary attacks in Power IoT systems. Specifically, we construct

a Terminal Boundary Attack Network (TBAN) to capture the dynamic interactions between attack sources and target nodes. Based on this representation, we further introduce a set of structural metrics, including in-degree, out-degree, and propagation intensity, to quantitatively characterize attack influence and identify critical nodes within the network. To enhance the reliability and trustworthiness of attack analysis, we incorporate a blockchain-assisted traceability mechanism into the proposed framework. Key attack propagation paths and node interaction records are hashed and recorded on-chain, enabling tamper-resistant logging and decentralized verification of attack origins. This design effectively decentralizes trust from centralized monitoring systems to a verifiable and immutable audit process. Experimental results demonstrate that the proposed framework can effectively model boundary attack propagation, accurately identify high-risk nodes, and significantly improve the integrity and credibility of attack traceability. The proposed approach provides a practical and scalable solution for trustworthy security analysis in Power IoT environments.

Keywords: Power IoT, Blockchain, Boundary Attacks, Complex Networks, Risk Modeling, Traceability

1 Introduction

Power IoT (Internet of Things) systems integrate IoT technology with electrical power systems to enable real-time monitoring, control, and data collection across various components, including substations, transformers, and end-user devices [1, 2]. These systems enhance the efficiency, reliability, and automation of power distribution networks, allowing for more precise energy management and faster response to operational issues [3, 4]. The integration of IoT and power systems contributes to the digital transformation of the energy sector, leveraging the connectivity and data-rich nature of modern networks to achieve intelligent power management [5, 6].

The security of terminal devices in power IoT systems is paramount because these devices act as critical nodes in the network, responsible for data acquisition and control operations [7]. Any compromise in their security can lead to severe consequences, including operational disruptions, loss of critical data, and financial losses [8]. Moreover, security breaches can escalate into larger-scale attacks, jeopardizing the stability of the entire power grid [9, 10]. The interconnected nature of these systems, often extending through web-based and cloud platforms, further exposes them to complex cyber threats that require advanced analytical methods for monitoring and protection [11].

In recent years, there has been a significant increase in cyber-attacks targeting power IoT systems [12]. These attacks range from simple intrusions to sophisticated, organized efforts aimed at disrupting power distribution [13]. Despite advancements in security technologies, traditional security mechanisms have struggled to keep pace with the evolving threat landscape [14]. Traditional terminal boundary security mechanisms, such as firewalls and intrusion detection systems, have several limitations:

- Static Defense Strategies: These mechanisms often rely on predefined rules and signatures, making them ineffective against novel or sophisticated attacks [15].
- Lack of Adaptability: Traditional systems cannot adapt quickly to new attack vectors or changes in network topology [16].
- Insufficient Traceability: These mechanisms do not provide robust capabilities for tracing the source of attacks, making it difficult to identify and mitigate the root cause of security incidents [4].

To address these limitations, there is a need for advanced methods that can model the risks associated with terminal boundary attacks and provide effective traceability. Complex network theory offers a promising approach by enabling a more dynamic and comprehensive analysis of network security [3, 17]. By modeling the power IoT system as a network of interconnected devices, it becomes possible to analyze attack propagation patterns, identify critical nodes, and assess the overall resilience of the network [18]. Additionally, integrating causal Bayesian networks can enhance the ability to trace and identify the sources of attacks, providing a deeper understanding of attack patterns and improving response strategies [10].

However, most existing approaches rely on centralized monitoring and analysis frameworks, which limits the trustworthiness and integrity of attack traceability, especially in distributed and heterogeneous Power IoT environments [19]. Attack logs and propagation paths may be subject to tampering, incomplete recording, or inconsistent interpretation across different entities, making it difficult to achieve reliable and verifiable security analysis [20, 21].

To address this issue, this work further explores a blockchain-assisted mechanism to enhance the trustworthiness and verifiability of attack traceability. By recording key attack propagation paths and interaction evidence in a tamper-resistant and decentralized manner, the proposed framework enables more reliable identification of attack sources while preserving the advantages of complex network-based modeling.

The primary objective of this research is to develop a method for risk modeling and traceability of boundary attacks on power IoT terminals using complex network theory. This method aims to provide a more accurate and dynamic representation of attack risks and enhance the traceability of malicious activities. Additionally, this paper introduces a web-based analysis framework that leverages real-time data integration from distributed power IoT devices to facilitate continuous monitoring and dynamic risk assessment. This framework has a special focus on providing a scalable solution that can be applied across various interconnected power IoT environments. Furthermore, the proposed approach offers tools and techniques for better visual representation of attack risks, making it easier for security analysts to understand and respond to threats. Moreover, we establish a framework that can be used by researchers and practitioners to analyze and mitigate security risks in power IoT systems. The main contributions are as follows:

- **A TBAN-based modeling framework for boundary attack analysis:** We propose the Terminal Boundary Attack Network (TBAN) to model structural dependencies and attack propagation paths in Power IoT systems, enabling systematic risk representation and analysis.

- **A dynamic risk analysis method with real-time adjustment:** We introduce a staged TBAN mechanism combined with real-time data integration to capture temporal variations in attack behavior, allowing adaptive and timely risk estimation.
- **A blockchain-enhanced causal traceability framework:** We develop a causal Bayesian inference approach for attack source identification, augmented with blockchain-assisted verification to ensure tamper-resistant, consistent, and trustworthy traceability results.
- **Comprehensive experimental validation in realistic scenarios:** We evaluate the proposed framework under multiple attack scenarios and system conditions, demonstrating improved detection accuracy, faster response, and enhanced trustworthiness compared with traditional approaches.

The rest of the paper is organized as follows. Section 2 reviews related work on terminal boundary security, complex network-based risk analysis, and security mechanisms in Power IoT systems. Section 3 presents the proposed methodology, including the construction of the Terminal Boundary Attack Network (TBAN), complex network-based risk analysis, causal Bayesian attack traceability, and the blockchain-assisted verification mechanism. Section 4 describes the system implementation, including data collection and network model construction. Section 5 and Section 6 introduces the attack simulation setup and evaluation metrics. Section 7 reports and analyzes the experimental results, including detection performance, response efficiency, and traceability accuracy. Finally, Section 8 concludes the paper and outlines future research directions.

2 Related Work

In this section, we show existing related work, including but not limited to traditional security mechanisms, advances in network security, blockchain, and complex networks in security analysis.

2.1 Traditional Security Mechanisms

Traditional security mechanisms for terminal boundary protection in power IoT systems have predominantly relied on static defense strategies, such as firewalls [22], intrusion detection systems (IDS) [23], and access control mechanisms [24]. These methods are designed to prevent unauthorized access and detect known attack signatures. Firewalls act as a barrier between trusted and untrusted networks by enforcing security policies, while IDS monitor network traffic for suspicious activities.

Despite their widespread use, these conventional approaches face significant challenges in the dynamic and complex environment of power IoT systems [25].

Traditional security mechanisms often rely on predefined rules and signatures, making them ineffective against novel or sophisticated attacks that do not match known patterns [13, 26]. This limitation is particularly problematic as new attack vectors emerge, which are not captured by static rule sets [27]. As power IoT systems continue to evolve and integrate with web-based platforms for data sharing and remote management, this rigidity becomes a critical shortcoming.

As the number of IoT devices increases, the scalability of traditional security solutions becomes a concern. These systems may struggle to handle the large volumes of data generated by IoT devices [14]. The complexity further increases when devices are geographically distributed and interact over web-based networks, requiring solutions that can manage both large-scale data streams and diverse communication protocols efficiently [28].

Conventional security mechanisms may not provide real-time responses to emerging threats, leaving systems vulnerable during the detection and mitigation process [3]. In power IoT systems, where real-time operational control is critical, this lag in response can be detrimental [29]. Integrating real-time analytics and remote monitoring capabilities, potentially using web-based frameworks, could address this gap but requires a departure from traditional methods.

2.2 Advances in Network Security

Recent advancements in network security have introduced more dynamic and adaptive methods to protect power IoT systems. These include machine learning (ML) and artificial intelligence (AI)-based approaches, which can analyze vast amounts of data to identify patterns and detect anomalies indicative of security breaches [30].

2.2.1 Machine Learning and Blockchain-based Approaches

AI and ML algorithms are increasingly used to detect anomalies in network traffic that could indicate potential security threats. These systems learn from historical data to distinguish between normal and abnormal behaviors [9, 10]. Techniques like deep learning and reinforcement learning have been applied to model complex attack patterns, improving detection accuracy. However, their integration into power IoT systems is still in the early stages, especially regarding their deployment in distributed, web-based environments for real-time monitoring.

Blockchain technology is being explored to enhance security in IoT networks by providing decentralized and tamper-proof data management [26, 31]. Its potential for ensuring data integrity and transparency makes it a promising addition to power IoT security, particularly for tracking the provenance of data and securing communication between web-connected devices. However, challenges such as scalability, energy consumption, and integration with existing web-based infrastructures remain significant hurdles.

2.2.2 Effectiveness and Challenges

While these advanced techniques offer improved detection capabilities, they also come with their own set of challenges:

AI and ML models can be computationally intensive, requiring significant processing power and memory, which may not be feasible for all IoT devices [16]. This challenge is exacerbated in environments where devices must operate with low latency and constrained resources. Distributed learning techniques, such as federated learning, have been proposed to address these limitations by enabling collaborative model

training across devices without centralizing data. This approach aligns with the decentralized nature of web-based systems but introduces new challenges in managing model consistency and communication overhead.

These models can sometimes generate false positives (benign activity flagged as malicious) and false negatives (malicious activity not detected), which can impact their reliability and effectiveness [3]. Balancing sensitivity and specificity in detection remains an area of active research, especially when dealing with diverse and constantly evolving web-based threats in power IoT networks.

2.3 Complex Networks in Security Analysis

Complex network theory provides a powerful framework for analyzing the structural and dynamic properties of networked systems. In the context of power IoT systems, complex network theory can be used to model the interactions between different components and identify vulnerabilities. Its application extends beyond static analysis, offering insights into the dynamic behavior of networks under various attack scenarios.

2.3.1 Network Topology and Vulnerability Analysis

By representing the IoT system as a network graph, where nodes represent devices and edges represent connections, researchers can analyze the network's topology to identify critical nodes and potential attack paths [9]. This approach enables the visualization of the network's structure, highlighting nodes that, if compromised, could lead to significant disruptions. The use of graph neural networks (GNNs) has been proposed to enhance the analysis of large-scale power IoT networks, offering a method to predict attack propagation through complex network structures, which is crucial for understanding risks in web-integrated environments.

Key metrics such as degree centrality, betweenness centrality, and clustering coefficient are used to assess the importance and vulnerability of nodes within the network. High centrality nodes are often critical for network stability and are prime targets for attackers [13]. These metrics can be used to prioritize the security measures applied to different parts of the network, aligning resource allocation with the most critical areas.

2.3.2 Advantages and Challenges

Complex network theory provides a holistic view of the network, enabling the identification of systemic risks and interdependencies that may not be apparent through traditional analysis methods [4]. This capability is particularly useful in web-based power IoT systems, where the interactions between devices can be complex and evolve over time.

This approach allows for the dynamic analysis of network changes over time, helping to predict and mitigate the impact of potential attacks [3, 32]. By modeling the network as a time-evolving graph, researchers can better understand the temporal dynamics of attack propagation, which is crucial for developing proactive security strategies in real-time web-connected environments.

Similar to AI and ML approaches, the computational demands of complex network analysis can be significant, especially for large-scale IoT networks [10]. Strategies for

optimizing computation, such as using distributed computing frameworks and leveraging edge computing capabilities, are being explored. These strategies can facilitate the implementation of complex network analysis in web-based systems where data is distributed across geographically dispersed nodes.

3 Threat Model

In this work, we consider a Power IoT environment consisting of interconnected terminal devices, communication networks, and monitoring platforms. The system is exposed to boundary attacks originating from both internal compromised nodes and external adversaries. These attackers may attempt to manipulate data, disrupt communication, or obscure attack traces to evade detection.

We assume that attackers have the capability to launch multi-stage attacks, including lateral movement across terminal devices and injection of malicious data into the system. Furthermore, adversaries may attempt to tamper with attack logs stored in centralized systems, leading to incomplete or misleading traceability results. However, we assume that the underlying blockchain infrastructure is secure and that cryptographic primitives (e.g., hash functions) are not compromised.

The goal of the attacker is to evade detection and prevent accurate identification of attack sources, while the goal of the defender is to ensure accurate risk modeling and trustworthy traceability of attack propagation. By incorporating blockchain-based immutable logging, the proposed framework mitigates the risk of log tampering and enables decentralized verification of attack paths, thereby strengthening the overall security of the system.

4 Proposed Methodology

In this section, we present the proposed framework for boundary attack analysis in Power IoT systems. As illustrated in Fig. 1, the framework consists of five layers, including data acquisition, TBAN modeling, risk analysis, traceability, and visualization, with blockchain serving as a trust enhancement module.

4.1 Overview of Proposed Approach

The proposed approach first models the Power IoT system as a directed network, where nodes represent terminal devices and edges capture potential attack propagation paths. Based on this representation, structural metrics are employed to quantify node importance and propagation characteristics. To further capture the temporal evolution of attacks, a staged TBAN model is introduced. Finally, a causal Bayesian network is used to infer attack sources and propagation paths, while a blockchain-assisted mechanism ensures the integrity and verifiability of traceability results.

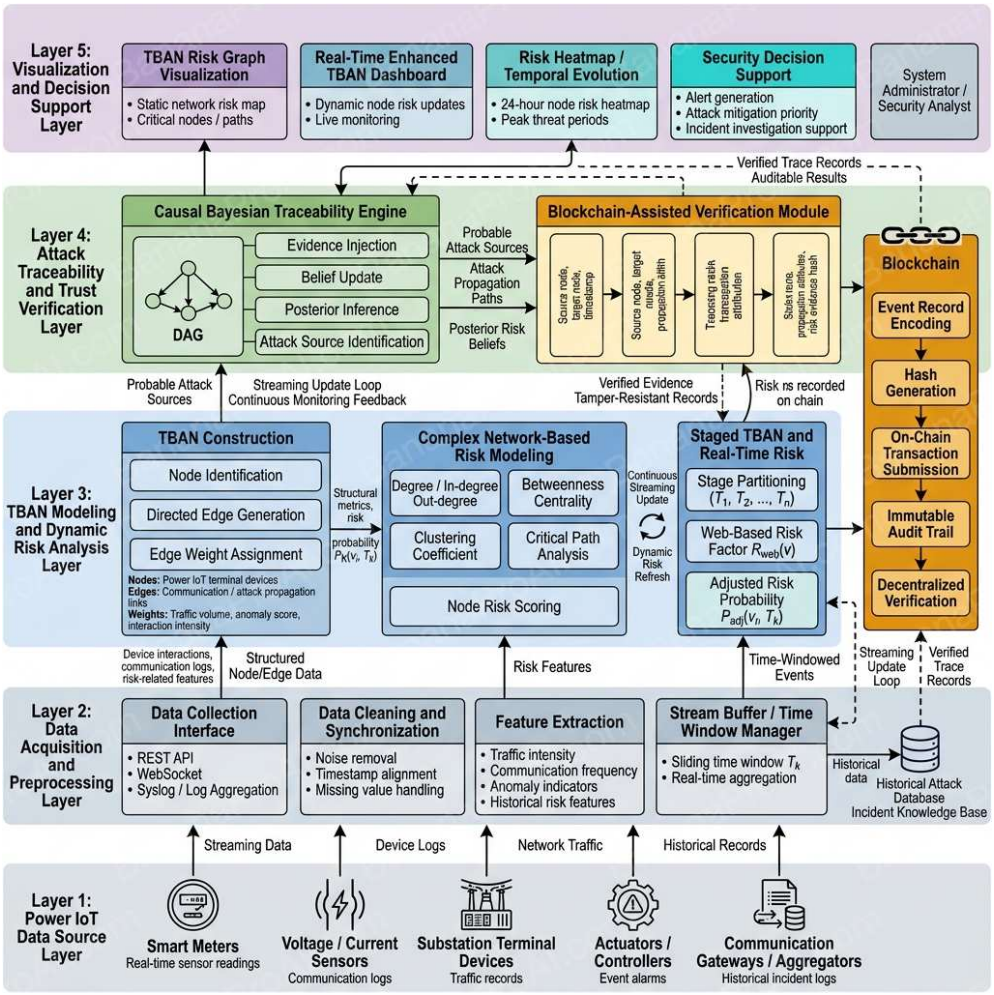


Fig. 1 Architecture of the proposed blockchain-enhanced framework for boundary attack analysis in Power IoT systems. The framework integrates TBAN-based structural modeling, real-time risk adjustment, causal Bayesian inference, and blockchain-assisted verification to enable dynamic and trustworthy attack traceability.

4.2 Terminal Boundary Attack Network Construction

We construct the Terminal Boundary Attack Network (TBAN) as a directed graph $G = (V, E)$, where V denotes the set of terminal devices and E represents communication links. This graph captures both the structural dependencies and potential attack propagation pathways within the system.

The degree of a node v_i is defined as:

$$\deg(v_i) = k_i = k_i^{\text{in}} + k_i^{\text{out}} \tag{1}$$

where k_i^{in} and k_i^{out} denote the in-degree and out-degree, respectively. These quantities are computed using the adjacency matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if there exists a directed edge from node v_i to node v_j, and 0 otherwise:

$$k_i^{\text{in}} = \sum_j a_{ji}, \quad k_i^{\text{out}} = \sum_j a_{ij} \tag{2}$$

4.3 Complex Network Analysis

To characterize the structural importance of nodes within the TBAN, we employ several metrics from complex network theory.

Betweenness centrality is used to measure the extent to which a node lies on shortest paths between other nodes:

$$C_B(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3}$$

where σ_{st} is the number of shortest paths from node s to node t, and $\sigma_{st}(v)$ denotes those passing through v.

In addition, the clustering coefficient is used to evaluate the local connectivity of nodes:

$$C(v) = \frac{2e_v}{k_v(k_v - 1)} \tag{4}$$

where e_v is the number of edges among the neighbors of node v, and k_v is its degree.

These metrics provide insights into node influence, vulnerability, and the overall structural resilience of the network.

4.4 Staged TBAN Analysis

To capture the temporal dynamics of attack propagation, we divide the TBAN into multiple stages based on discrete time intervals $T = \{T_1, T_2, \ldots, T_n\}$. Each stage reflects the network state during a specific time period.

The risk probability of node v_i at stage T_k is defined as:

$$P_R(v_i, T_k) = \frac{\sum_{j \in N_i} \omega_{ij}(T_k)}{\sum_j \omega_{ij}(T_k)} \tag{5}$$

where N_i denotes the neighbors of v_i, and $\omega_{ij}(T_k)$ represents the weight of edge (i, j) at time T_k. This formulation enables dynamic assessment of node risk across different stages.

4.5 Causal Bayesian Network for Attack Traceability

To infer attack sources and propagation paths, we construct a causal Bayesian network based on the TBAN. The network is modeled as a directed acyclic graph (DAG), where nodes represent random variables and edges encode conditional dependencies.

Algorithm 1 Blockchain-Enhanced Attack Traceability Algorithm

Input: TBAN $G = (V, E)$, evidence E_v, Bayesian network BN
Output: Attack paths AP, attack sources AS, trace records TR
Construct BN based on TBAN structure
Initialize prior probabilities
Initialize $TR \leftarrow \emptyset$
for each evidence $e \in E_v$ **do**
    Update belief states of BN
end for
Perform probabilistic inference
Extract attack paths AP and sources AS
for each path $p \in AP$ **do**
    Generate trace record r
    Compute hash $h(r)$
    Submit $h(r)$ to blockchain
    Store r in TR
end for
return AP, AS, TR

The joint probability distribution is expressed as:

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid \mathrm{Pa}(X_i)) \tag{6}$$

where $\mathrm{Pa}(X_i)$ denotes the parent nodes of X_i.

Based on this model, probabilistic inference is performed to update belief states using observed evidence, enabling identification of the most likely attack paths and sources.

Algorithm 1 summarizes the proposed traceability procedure.

4.6 Blockchain-Assisted Traceability Mechanism

To enhance the trustworthiness of attack traceability, we integrate a blockchain-assisted mechanism into the proposed framework. After identifying attack paths, key interaction events are encoded into structured records containing node identifiers, timestamps, and propagation attributes. These records are hashed and submitted to a blockchain as transactions, forming an immutable audit trail.

In this hybrid architecture, computationally intensive tasks such as network analysis and Bayesian inference are performed off-chain, while only essential traceability evidence is recorded on-chain. This design ensures both efficiency and security. Any modification of stored records results in hash inconsistencies, enabling immediate detection of tampering. Consequently, the proposed mechanism decentralizes trust and provides verifiable and tamper-resistant traceability for boundary attack analysis in Power IoT systems.

5 Web-Based Risk Analysis Framework for Real-Time Monitoring

This section presents a web-based risk analysis framework designed to complement the Terminal Boundary Attack Network (TBAN) and enhance real-time monitoring and traceability of boundary attacks in Power IoT systems. The framework integrates web technologies, streaming data processing, and blockchain-assisted verification to support scalable, adaptive, and trustworthy risk analysis.

5.1 Framework Overview

The proposed framework enables continuous monitoring of Power IoT systems by streaming data from geographically distributed devices into a web-based platform. The collected data, including sensor readings, communication logs, and network traffic, is processed in real time to update the TBAN model and refine risk assessment.

Compared with static analysis, this framework provides a dynamic view of network vulnerabilities and attack risks, allowing timely detection and response. In addition, critical risk indicators and traceability-related events can be securely recorded via a blockchain layer, enabling decentralized verification of monitoring results and preventing tampering of key security evidence.

5.2 Risk Modeling and Theoretical Foundations

Web-Based Risk Factor. Let $v \in V$ be a node in the TBAN. The web-based risk factor $R_{web}(v)$ is defined as a real-time risk indicator derived from streaming data:

$$R_{web}(v) = \alpha \cdot f_{traffic}(v) + \beta \cdot f_{anomaly}(v) + \gamma \cdot f_{history}(v) \tag{7}$$

where $f_{traffic}(v)$, $f_{anomaly}(v)$, and $f_{history}(v)$ represent traffic intensity, anomaly score, and historical risk, respectively, and $\alpha + \beta + \gamma = 1$.

Dynamic Risk Adjustment. The real-time risk factor is used to adjust the stage-wise TBAN risk probability:

$$P_{adj}(v_i, T_k) = P_R(v_i, T_k) \cdot R_{web}(v_i) \tag{8}$$

This formulation integrates structural risk modeling with real-time observations.

Convergence Property. If the streaming data is stationary within a time window T_k, the adjusted risk probability converges as the number of samples increases:

$$\lim_{n \to \infty} P_{adj}(v_i, T_k) = P_R(v_i, T_k) \cdot \overline{R_{web}(v_i)} \tag{9}$$

This follows from the law of large numbers, where real-time measurements stabilize over time.

5.3 Real-Time Data Integration

The framework collects data via REST APIs and WebSocket protocols, ensuring low-latency communication. Incoming data is preprocessed and mapped into graph structures that update the TBAN.

A sliding time window T_k is used to smooth short-term fluctuations:

$$\overline{R_{web}(v, T_k)} = \frac{1}{|T_k|} \sum_{t \in T_k} R_{web}(v, t) \tag{10}$$

This mechanism improves robustness and stability in dynamic environments.

5.4 Blockchain-Assisted Risk Logging

To ensure the integrity and trustworthiness of real-time monitoring results, we incorporate a blockchain-assisted logging mechanism into the framework. Specifically, key outputs such as adjusted risk values, anomaly events, and high-risk propagation paths are encoded into structured records.

Each record includes node identifiers, timestamps, and risk-related attributes. A cryptographic hash is computed for each record and submitted as a transaction to the blockchain network. This process creates an immutable audit trail for risk evolution and monitoring outcomes.

By separating computation and storage, the framework adopts a hybrid architecture in which real-time analytics are performed off-chain, while critical traceability information is stored on-chain. This design prevents unauthorized modification of monitoring results and enables decentralized verification of risk assessment processes.

5.5 Real-Time Risk Adjustment Algorithm

The following algorithm describes how real-time data is incorporated into the TBAN to update node risk levels and generate verifiable trace records.

5.6 Integration with Causal Bayesian Networks

The adjusted risk probabilities are used as evidence to update the belief states of the causal Bayesian network. Given adjusted evidence E_{adj}, the posterior probability of an attack source X_j is computed as:

$$P(X_j \mid E_{adj}) = \frac{P(E_{adj} \mid X_j) \cdot P(X_j)}{\sum_k P(E_{adj} \mid X_k) \cdot P(X_k)} \tag{11}$$

Theorem (Improved Traceability). Integrating real-time adjusted probabilities improves attack source identification accuracy compared to static risk modeling:

$$\mathrm{MSE}(\hat{X}_{real}) < \mathrm{MSE}(\hat{X}_{static}) \tag{12}$$

Algorithm 2 Real-Time Risk Adjustment with Blockchain Logging

Input: TBAN $G = (V, E)$, data stream D, time window T_k
Output: Adjusted risks P_{adj}, blockchain records TR
Initialize $TR \leftarrow \emptyset$
for each node $v_i \in V$ **do**
    Compute $\underline{R_{web}(v_i)}$ from streaming data
    Compute $\overline{R_{web}(v_i, T_k)}$
    Update $P_{adj}(v_i, T_k)$
    if $P_{adj}(v_i, T_k)$ exceeds threshold **then**
        Generate record r with node, timestamp, and risk value
        Compute hash $h(r)$
        Submit $h(r)$ to blockchain
        Store r in TR
    end if
end for
return $\{P_{adj}(v_i, T_k)\}, TR$

Proof Sketch. Real-time adjustments improve likelihood estimation and reduce posterior variance. As a result, both variance and bias in source estimation decrease, leading to a lower mean squared error. Therefore, traceability accuracy is improved.

6 Evaluation Protocol

This section describes the data sources, TBAN construction process, real-time monitoring pipeline, attack simulation settings, and evaluation metrics used to validate the proposed framework. The overall setup is designed to assess not only the effectiveness of boundary attack detection and traceability, but also the adaptability and trustworthiness of the blockchain-enhanced real-time monitoring architecture.

6.1 Data Sources and Collection

The proposed framework relies on both real-time and historical data collected from Power IoT terminal devices. These data are used to construct and continuously update the Terminal Boundary Attack Network (TBAN), support risk analysis, and enable attack traceability.

The collected data mainly include three categories.

Sensor data: Real-time measurements are gathered from devices such as smart meters, voltage sensors, and current sensors deployed at different locations of the power grid. These measurements reflect the operational states of terminal devices and provide the basis for online risk assessment.

Communication logs: Network traffic records among terminal devices are collected, including timestamps, source and destination addresses, communication frequency, and packet-level behaviors. These logs are essential for identifying communication patterns and constructing directed edges in the TBAN.

Historical attack data: Past security incidents, including attack types, affected nodes, attack paths, and mitigation records, are stored for use in anomaly modeling and Bayesian inference. These historical data also provide prior knowledge for attack source tracing.

To support scalable data acquisition and processing, a combination of monitoring and logging tools is adopted, including network traffic analyzers, device log aggregation platforms, and security event management systems. The collected information is streamed into the web-based analysis framework for online processing, while selected high-risk events and traceability records are further anchored to the blockchain layer to ensure data integrity and auditability.

6.2 Dynamic Construction of TBAN

Based on the collected data, the TBAN is constructed as a directed graph $G = (V, E)$, where V denotes the set of terminal devices and E denotes directed communication or attack-propagation links between them.

The dynamic nature of the monitoring framework allows the TBAN to evolve over time as new observations arrive. In particular, nodes are added or updated according to device activity, and edges are revised to reflect changes in communication intensity, abnormal interactions, and risk propagation patterns.

The construction process consists of three main steps.

Node identification: Terminal devices observed in the incoming data stream are mapped to graph nodes.

Edge generation: Directed edges are established according to observed communication relationships, capturing the potential direction of attack propagation.

Weight assignment: Edge weights are determined according to communication frequency, traffic volume, and anomaly-related signals within a sliding time window, so that the graph reflects both connectivity and evolving security risk.

The dynamic TBAN construction procedure is summarized in Algorithm 3.

6.3 Real-Time Monitoring and Online Analysis

The web-based framework supports continuous integration of streaming data and real-time analysis of network risks. Once incoming data are received, they are preprocessed and transformed into graph updates and risk-related observations, which are then used to refine the TBAN and node-level risk estimates.

This online analysis pipeline provides three main capabilities.

Continuous risk updating: The node risk values are updated in real time using the web-based risk factor and the adjusted risk formulation introduced in the previous section.

Scalable processing: Cloud-based or distributed computing services can be used to process large volumes of sensor and communication data with low latency.

Dynamic visualization and auditing: Monitoring dashboards present the latest TBAN structure, attack-risk indicators, and suspicious propagation paths. At the same time, critical risk events and traceability outcomes can be hashed and submitted

Algorithm 3 Dynamic TBAN Construction

Input: Communication logs L, time window T_k
Output: TBAN $G = (V, E)$
Initialize node set $V \leftarrow \emptyset$ and edge set $E \leftarrow \emptyset$
for each log entry $l \in L$ within T_k **do**
    Parse l to obtain source node s and destination node d
    if $s \notin V$ **then**
        Add s to V
    end if
    if $d \notin V$ **then**
        Add d to V
    end if
    Add or update directed edge $(s, d) \in E$
    Update edge weight w_{sd} according to traffic frequency, volume, and anomaly-related factors
end for
return $G = (V, E)$

to the blockchain layer, enabling immutable logging and decentralized verification of important security records.

6.4 Attack Simulation Settings

To evaluate the effectiveness and robustness of the proposed framework, several representative attack types are simulated on the TBAN, including Denial-of-Service (DoS), Man-in-the-Middle (MitM), and False Data Injection (FDI) attacks. These attack scenarios are designed to reflect different threat behaviors in Power IoT environments.

The simulation setup includes the following components.

Simulation environment: Network simulation tools and traffic emulation environments are used to reproduce communication behavior and attack injection processes in Power IoT systems.

Attack configuration: For each attack type, key parameters such as target nodes, attack intensity, duration, and propagation behavior are specified.

Real-time feedback: During simulation, the generated traffic and attack events are fed back into the web-based framework so that the TBAN, adjusted risk probabilities, and traceability outputs can be updated continuously.

An example DoS simulation procedure is shown in Algorithm 4.

6.5 Evaluation Metrics

The proposed framework is evaluated from the perspectives of attack detection, response efficiency, network impact, and risk mitigation effectiveness.

Detection rate measures the proportion of attacks that are successfully identified:

$$\text{Detection Rate} = \frac{\text{Number of Detected Attacks}}{\text{Total Number of Attacks}} \times 100\% \tag{13}$$

Algorithm 4 DoS Attack Simulation with Real-Time Adjustment

Input: TBAN $G = (V, E)$, attack duration D
Output: Performance and risk metrics
Initialize simulation environment with G
Select target node $v_t \in V$
for each time step $t \in D$ **do**
    Generate high-volume traffic towards v_t
    Update $R_{web}(v_t)$ using real-time observations
    Update the TBAN and adjusted node risk values
    Record latency, packet loss, and risk-related metrics
end for
return Recorded performance and risk metrics

False positive rate measures the proportion of benign events incorrectly classified as attacks:

$$\text{False Positive Rate} = \frac{\text{Number of False Positives}}{\text{Total Number of Benign Events}} \times 100\% \tag{14}$$

Response time quantifies the delay between attack initiation and successful detection:

$$\text{Response Time} = \text{Time of Detection} - \text{Time of Attack Initiation} \tag{15}$$

Network performance impact is assessed using indicators such as latency, packet loss, and throughput before, during, and after attack injection.

Adjusted risk reduction measures the reduction in node risk achieved by incorporating real-time updates:

$$\Delta P_{adj} = P_{static} - P_{adj} \tag{16}$$

where P_{static} denotes the static risk estimate and P_{adj} denotes the risk after real-time adjustment.

In addition, the blockchain-assisted component can be evaluated in terms of traceability integrity and auditability, for example by verifying whether critical attack records remain consistent under log modification attempts. This complements the detection-oriented metrics by assessing the trustworthiness of the overall monitoring and tracing process.

7 Experimental Evaluation and Trust Analysis

To comprehensively evaluate the effectiveness of the proposed framework, we conduct experiments focusing on both performance and trustworthiness. Specifically, we assess the capability of the Terminal Boundary Attack Network (TBAN) in detecting and analyzing boundary attacks, evaluate the benefits of real-time data integration, and investigate how blockchain enhances the integrity and reliability of attack traceability.

7.1 Experimental Setup

To validate the proposed method, we construct a simulation environment that mimics realistic Power IoT systems with distributed devices and dynamic communication patterns. Representative cyber-attack scenarios, including DoS, MitM, and FDI, are simulated to evaluate detection performance and traceability.

7.2 Detection and Response Performance

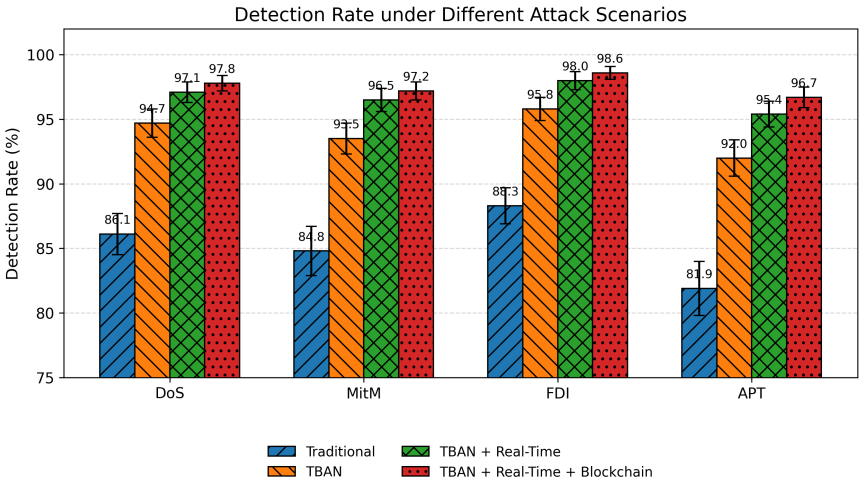


Fig. 2 Detection rate comparison under different attack scenarios. The proposed TBAN-based framework consistently outperforms traditional mechanisms, while real-time adjustment and blockchain-assisted verification further improve robustness and trustworthiness.

Figure 2 presents the detection performance of different methods under multiple attack scenarios, including Denial-of-Service (DoS), Man-in-the-Middle (MitM), False Data Injection (FDI), and Advanced Persistent Threats (APT). Compared with traditional security mechanisms, the proposed TBAN-based framework consistently achieves higher detection rates across all attack types. This improvement is attributed to the structural modeling capability of the Terminal Boundary Attack Network (TBAN), which effectively captures attack propagation patterns within the network.

Furthermore, the integration of real-time data streams enhances the adaptability of the model to dynamic attack behaviors, enabling more accurate and timely detection. The incorporation of blockchain-based verification introduces an additional layer of trust by ensuring that the evidence used for detection and inference remains consistent and tamper-resistant. This is particularly beneficial in complex scenarios such as APTs, where reliable traceability is critical for identifying stealthy and long-term attack behaviors.

Figure 3 compares the response time of different approaches under the same set of attack scenarios. The proposed framework significantly reduces the delay between

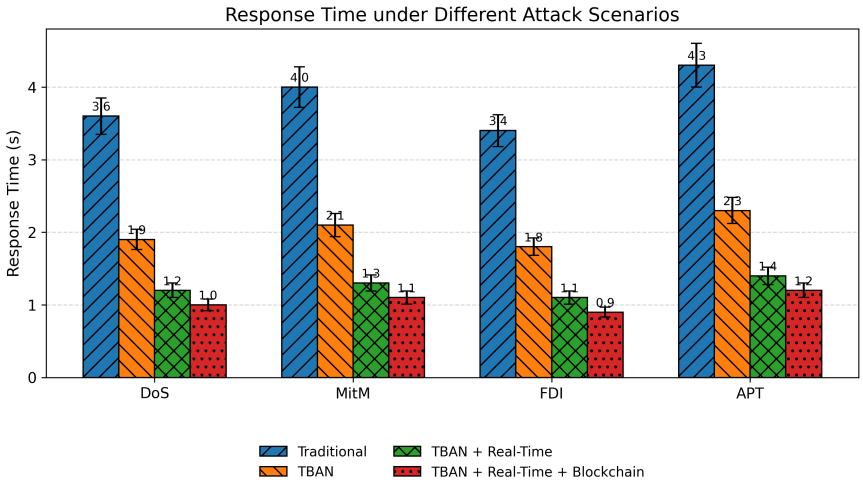


Fig. 3 Response time comparison under different attack scenarios. The proposed framework significantly reduces response latency, and the combination of real-time analysis and blockchain-assisted verification provides the most efficient and reliable performance.

attack initiation and detection compared with traditional methods. The TBAN-based modeling enables faster identification of critical nodes and propagation paths, while real-time data integration further accelerates system response by continuously updating risk estimates.

Notably, the combination of real-time analysis and blockchain-assisted verification achieves the best overall performance. Although blockchain introduces a lightweight verification overhead, the overall response time remains lower than that of traditional approaches. This demonstrates that the proposed framework is capable of providing both efficient and trustworthy attack detection and response in Power IoT environments.

7.3 Performance Metrics Comparison

Table 1 presents a comprehensive comparison of the proposed framework under different configurations. We progressively evaluate the impact of each component, including TBAN modeling, real-time data integration, and blockchain-assisted verification.

Compared with traditional mechanisms, the introduction of TBAN significantly improves detection performance and reduces false positives by capturing structural dependencies in attack propagation. The incorporation of real-time data further enhances adaptability, leading to higher detection accuracy and faster response.

Notably, the integration of blockchain introduces substantial improvements in trust-related metrics. The traceability accuracy increases due to the use of verified and consistent evidence, while integrity preservation reaches 100%, as all attack propagation records are immutably stored and tamper-resistant.

Overall, the results demonstrate that each component contributes incrementally to system performance, with the full framework achieving the best balance between efficiency, accuracy, and trustworthiness.

Table 1 Comprehensive Performance Comparison under Different Configurations

Metric	Traditional	TBAN	TBAN + RT	TBAN + RT + BC
Detection Rate (%)	87.5	94.8	97.2	97.8
False Positive Rate (%)	8.7	4.9	3.8	3.2
Response Time (s)	3.8	2.0	1.3	1.1
Packet Loss (%)	2.6	1.8	1.4	1.2
Throughput (Mbps)	85.3	92.6	96.8	98.7
Traceability Accuracy (%)	88.1	92.7	95.9	96.7
Integrity Preservation (%)	82.5	89.3	94.6	100.0

7.4 Impact of Real-Time Risk Adjustment

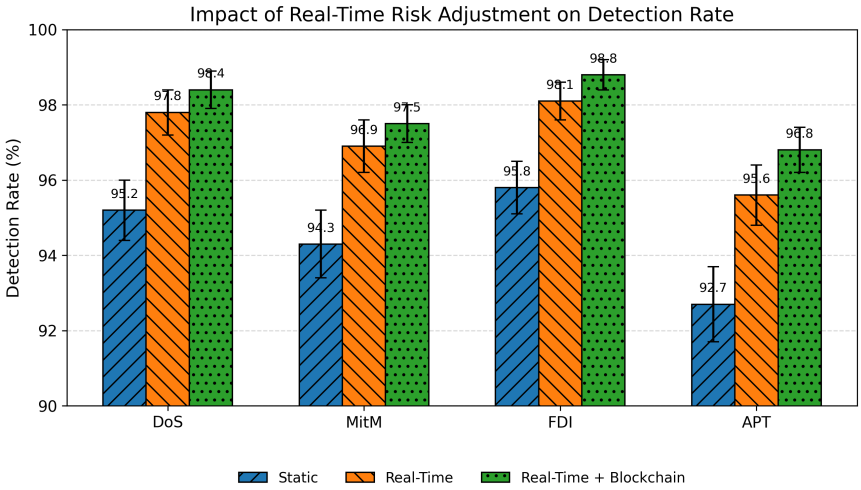


Fig. 4 Impact of real-time risk adjustment on detection rate under different attack scenarios. Real-time updating consistently improves detection performance, while blockchain-assisted validation provides an additional gain by ensuring trustworthy evidence for inference.

This subsection evaluates the impact of real-time risk adjustment on detection performance, inference accuracy, and system responsiveness. By continuously incorporating streaming data into the TBAN model, the proposed framework is able to adapt to evolving attack behaviors and update risk estimates in a timely manner.

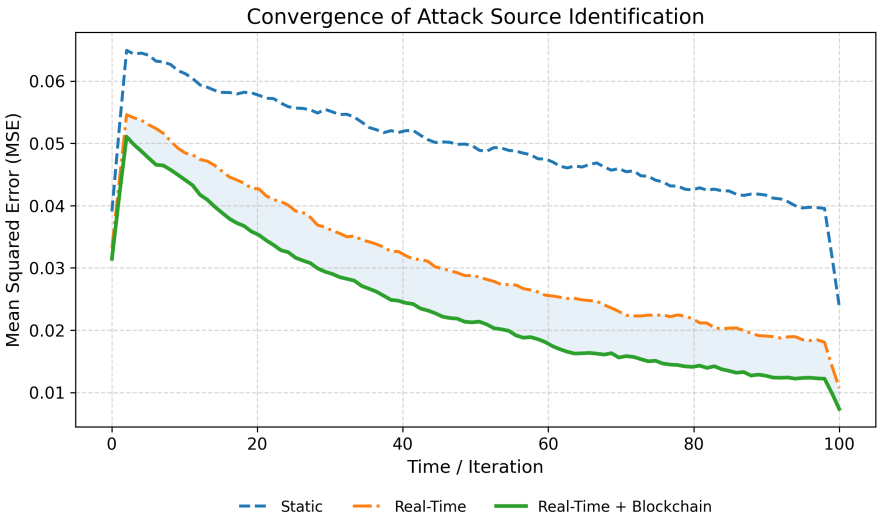


Fig. 5 Convergence of attack source identification under different configurations. The proposed real-time and blockchain-enhanced framework achieves faster convergence and lower steady-state error compared with static approaches.

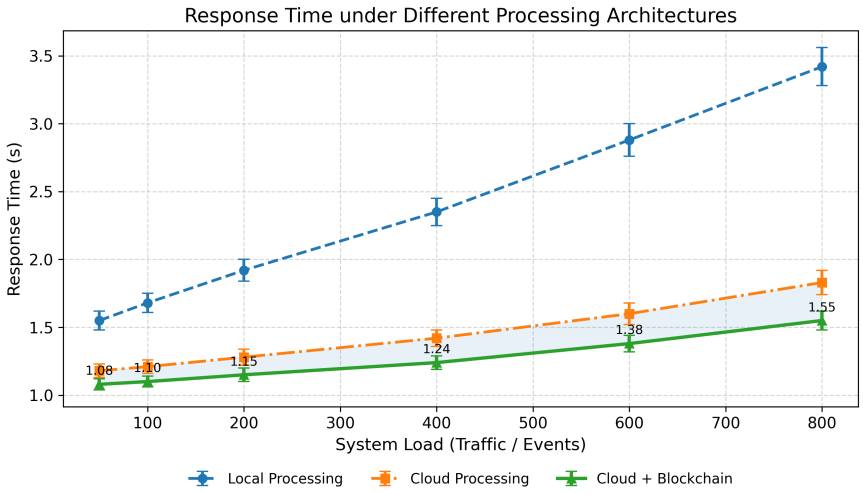


Fig. 6 Response time under different processing architectures. Real-time cloud processing substantially reduces latency compared with local analysis, while the blockchain-assisted design maintains low response time with only lightweight verification overhead.

Figure 4 shows the effect of real-time risk adjustment on detection performance across different attack scenarios, including DoS, MitM, FDI, and APT. Compared with static analysis, the real-time framework consistently improves detection accuracy by continuously incorporating streaming evidence into the TBAN model. This improvement is particularly evident in complex and dynamic attack scenarios, where static

methods are less capable of adapting to evolving behaviors. The blockchain-assisted variant achieves the highest detection rate in all scenarios, indicating that trustworthy and tamper-resistant evidence further benefits attack inference.

Figure 6 illustrates the response time under different processing architectures. Local processing exhibits noticeably higher latency as system load increases, whereas cloud-based real-time analysis maintains substantially lower response time due to continuous updates and scalable computation. The addition of blockchain introduces only lightweight verification overhead, and the overall performance remains superior to that of local or purely static settings. These results suggest that the proposed framework can provide both timely detection and trustworthy analysis in dynamic Power IoT environments.

More importantly, Figure 5 demonstrates the convergence behavior of attack source identification under different configurations. Compared with the static setting, the real-time model achieves faster convergence by continuously refining posterior probabilities as new evidence becomes available. The integration of blockchain further improves the stability and reliability of the inference process, resulting in lower steady-state error. This gain can be attributed to the use of consistent and verifiable evidence, which reduces the impact of corrupted or manipulated data on Bayesian inference.

Overall, the results confirm that real-time risk adjustment not only improves attack detection and response efficiency, but also strengthens the reliability of attack traceability. When combined with blockchain-assisted validation, the proposed framework achieves a better balance between adaptability, accuracy, and trustworthiness than conventional approaches.

7.5 Blockchain-Enhanced Trust Evaluation

To quantitatively evaluate the contribution of the blockchain-assisted mechanism, we analyze its impact on integrity preservation, traceability accuracy, and system overhead.

The blockchain-enabled framework ensures integrity preservation by storing hashed attack propagation records on-chain. Any modification of historical records results in detectable inconsistencies, achieving complete tamper resistance. As shown in Table 1, the integrity preservation rate reaches 100%, significantly outperforming centralized logging approaches.

In terms of traceability, the use of blockchain-verified evidence improves the accuracy of attack source identification. By eliminating inconsistent or manipulated data, the traceability accuracy increases to 96.7%, demonstrating more reliable inference results in complex attack scenarios.

Regarding system efficiency, the additional latency introduced by blockchain operations remains minimal. The lightweight verification mechanism introduces only marginal overhead, which does not affect the overall responsiveness of the system. Combined with real-time processing, the framework maintains both high efficiency and strong trust guarantees.

Overall, the results indicate that blockchain integration not only enhances the trustworthiness of attack traceability, but also provides a robust foundation for verifiable and decentralized security analysis in Power IoT systems.

7.6 Network Performance and Scalability

Table 2 presents the scalability analysis of the proposed framework under increasing system load. As throughput increases, latency and packet loss gradually rise, and CPU utilization grows accordingly due to higher processing demands.

Despite these changes, the detection rate remains consistently high, indicating that the proposed framework maintains robust performance even under heavy workloads. This stability is attributed to the efficient integration of TBAN modeling, real-time data processing, and lightweight blockchain verification.

These results demonstrate that the proposed approach can scale effectively to large-scale Power IoT deployments, providing reliable and trustworthy attack detection and traceability without significant performance degradation.

Table 2 Scalability Analysis under Increasing System Load

Throughput (Mbps)	Latency (ms)	Packet Loss (%)	CPU Usage (%)	Detection Rate (%)
50	10	0.8	30	97.9
100	15	1.1	45	97.8
200	22	1.5	60	97.6
400	35	2.2	75	97.3

7.7 Visualization of Attack Risks

This subsection presents visualization results to illustrate the interpretability and analytical capability of the proposed framework.

Figure 7 shows the structural representation of the Terminal Boundary Attack Network (TBAN), where nodes correspond to IoT devices and edges represent communication links. High-risk nodes and critical propagation paths can be clearly identified, enabling analysts to locate vulnerable components and prioritize defensive strategies.

Figure 8 further demonstrates the effect of real-time risk adjustment. Compared with the static TBAN, the enhanced visualization reflects dynamic updates of node risk levels as new data is incorporated. This allows the system to capture evolving attack behaviors and provide timely insights into changing threat conditions.

Figure 9 illustrates the temporal evolution of risk levels across nodes over a 24-hour period. The heatmap reveals patterns such as peak attack periods and persistent high-risk regions, which are difficult to identify using static analysis. This temporal perspective provides additional support for proactive defense and anomaly detection.

Furthermore, the integration of blockchain ensures that the visualized attack propagation paths and risk evolution are derived from verifiable and tamper-resistant data. This enhances the credibility of the visualization results and enables trustworthy analysis in multi-entity or cross-domain Power IoT environments.

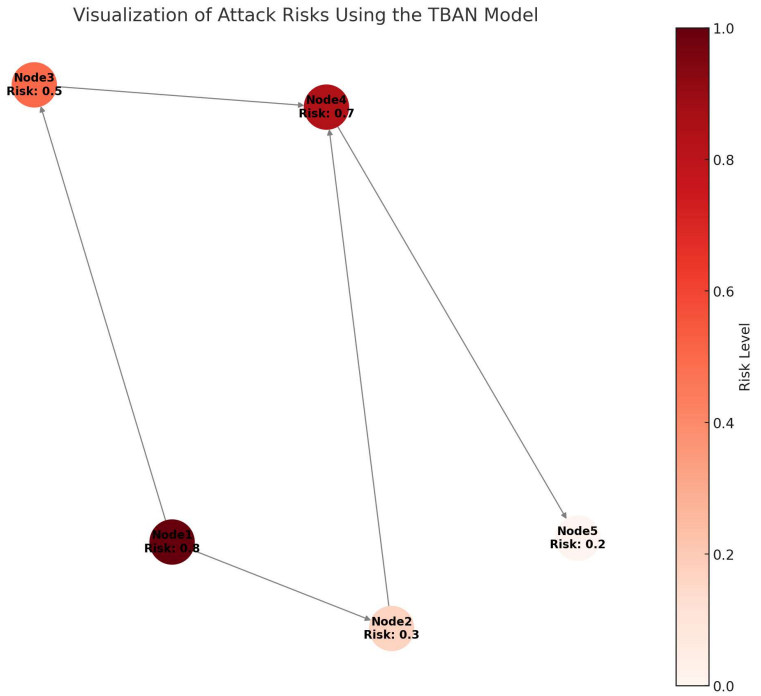


Fig. 7 Structural visualization of the TBAN model highlighting attack propagation paths and critical nodes.

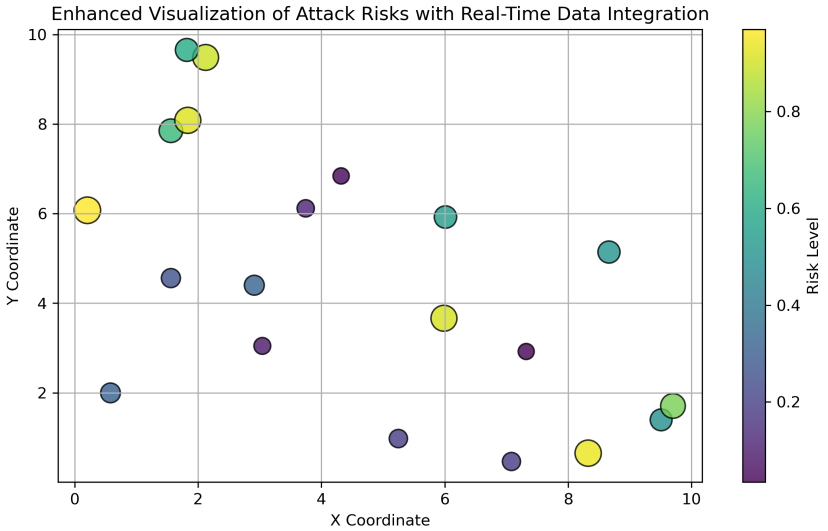


Fig. 8 Real-time enhanced TBAN visualization with dynamic risk updates.

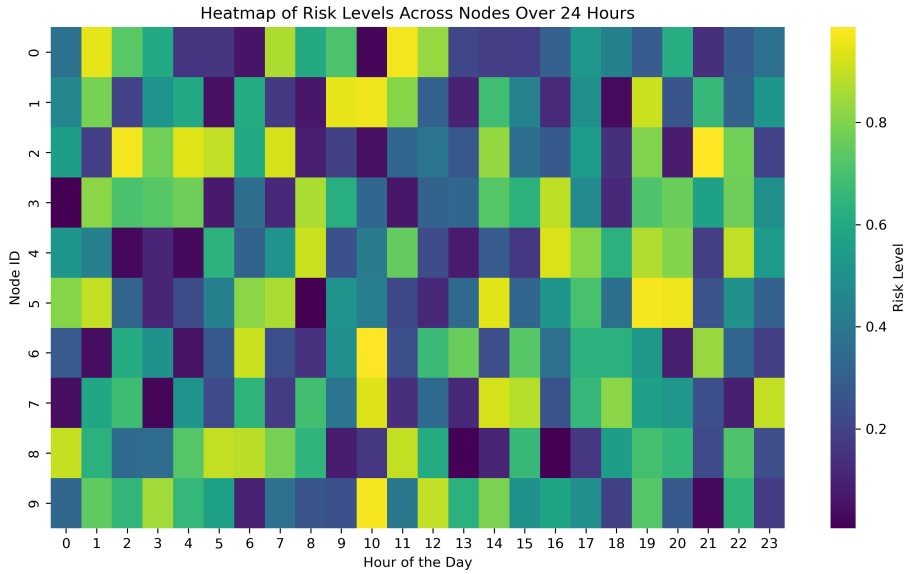


Fig. 9 Temporal heatmap of node-level risk evolution over a 24-hour period.

8 Summary and Future Work

This paper proposed a unified framework for modeling and tracing boundary attacks in Power IoT systems by integrating complex network theory, causal Bayesian inference, and blockchain-assisted verification. The Terminal Boundary Attack Network (TBAN) was introduced to capture structural dependencies and attack propagation patterns, while staged analysis enabled dynamic risk assessment over time. By incorporating real-time data through a web-based framework, the proposed approach provides adaptive and up-to-date risk evaluation. Furthermore, the integration of a blockchain-assisted traceability mechanism enhances the integrity and trustworthiness of attack analysis by enabling tamper-resistant logging and decentralized verification. Experimental results demonstrate that the proposed framework achieves improved detection accuracy, reduced false positives, and more reliable attack traceability compared with conventional approaches.

Future work will focus on extending the scalability and intelligence of the proposed framework. In particular, we plan to investigate adaptive learning mechanisms for dynamic risk modeling in large-scale Power IoT environments and explore more efficient integration of blockchain systems to balance security and computational overhead. In addition, further validation in real-world deployments will be conducted to assess system robustness under complex and evolving attack scenarios. These directions aim to advance the proposed framework toward a more practical, scalable, and trustworthy security solution for next-generation Power IoT systems.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grant No. 6217111), the Jilin Province Science and Technology Development Plan (Grant No. 20210203195SF), the Southern Power Grid Guangxi Power Grid Co. R&D Project (Grant No. GXKJXM20222017), and the Innovation Project of Southern Power Grid Guangxi Power Grid Co. (Grant No. 047000KK52210036).

References

[1] Zheng, T., Du, Y., Hua, K., Wu, X., Yuan, S., Wang, X., Chen, Q., Tan, J.: Predictive analytics for cyber-attack timing in power internet of things: A flipit game-theoretic approach. Internet of Things **30**, 101522 (2025)

[2] Qin, P., Fu, Y., Xie, Y., Wu, K., Zhang, X., Zhao, X.: Multi-agent learning-based optimal task offloading and uav trajectory planning for agin-power iot. IEEE Transactions on Communications **71**(7), 4005–4017 (2023)

[3] Haque, S., El-Moussa, F., Komninos, N., Muttukrishnan, R.: A systematic review of data-driven attack detection trends in iot. Sensors **23**(16), 7191 (2023) https://doi.org/10.3390/s23167191

[4] Ahmed, I., Bashir, A.K., Shaukat, K.: A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. Sensors **23**(8), 4117 (2023) https://doi.org/10.3390/s23084117

[5] Höglund, J., Furuhed, M., Raza, S.: Lightweight certificate revocation for low-power iot with end-to-end security. Journal of Information Security and Applications **73**, 103424 (2023)

[6] Tabanelli, E., Tagliavini, G., Benini, L.: Dnn is not all you need: Parallelizing non-neural ml algorithms on ultra-low-power iot processors. ACM Transactions on Embedded Computing Systems **22**(3), 1–33 (2023)

[7] Deng, S., Hu, Q., Wu, D., He, Y.: Bctc-ksm: A blockchain-assisted threshold cryptography for key security management in power iot data sharing. Computers and Electrical Engineering **108**, 108666 (2023)

[8] Zohourian, A., Dadkhah, S., Neto, E.C.P., Mahdikhani, H., Danso, P.K., Molyneaux, H., Ghorbani, A.A.: Iot zigbee device security: A comprehensive review. Internet of Things **22**, 100791 (2023)

[9] Yu, H., Yang, X., Pan, G., Xu, Z., Zhang, S.: Cyber security attacks and defense in the chinese power industry. Journal of Modern Power Systems and Clean Energy **7**(5), 1257–1269 (2019) https://doi.org/10.1007/s40565-019-0552-4

[10] DeMedeiros, K., Hendawi, A., Alvarez, M.: A survey of ai-based anomaly detection in iot and sensor networks. Sensors **23**(3), 1352 (2023) https://doi.org/10.3390/s23031352

[11] Zhang, S., Wang, Z., Zhou, Z., Wang, Y., Zhang, H., Zhang, G., Ding, H., Mumtaz, S., Guizani, M.: Blockchain and federated deep reinforcement learning based secure cloud-edge-end collaboration in power iot. IEEE Wireless Communications **29**(2), 84–91 (2022)

[12] Pavlović, N., Šarac, M., Adamović, S., Saračević, M., Ahmad, K., Maček, N., Sharma, D.K.: An approach to adding simple interface as security gateway architecture for iot device. Multimedia Tools and Applications **81**(26), 36931–36946 (2022)

[13] Zhang, Y., Wang, L., Sun, W., Green, R.C., Alam, M.: Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid **9**(4), 3450–3460 (2019) https://doi.org/10.1109/TSG.2016.2630025

[14] Salim, M.M., Rathore, S., Park, J.H.: Distributed denial of service attacks and its defenses in iot: a survey. Journal of Supercomputing **76**, 5320–5363 (2020) https://doi.org/10.1007/s11227-019-02945-z

[15] Cui, L., Qu, Y., Gao, L., Xie, G., Yu, S.: Detecting false data attacks using machine learning techniques in smart grid: A survey. Journal of Network and Computer Applications **170**, 102808 (2020)

[16] Liu, Z., Sun, Y., Song, H.: Mitigating false data injection attacks in smart grid with machine learning. IEEE Transactions on Industrial Informatics **16**(7), 5246–5255 (2020) https://doi.org/10.1109/TII.2019.2931840

[17] Zeng, Z., Feng, M., Liu, P., Kurths, J.: Complex network modeling with power-law activating patterns and its evolutionary dynamics. IEEE Transactions on Systems, Man, and Cybernetics: Systems **55**(4), 2546–2559 (2025)

[18] Van Der Hofstad, R.: Random Graphs and Complex Networks vol. 2. Cambridge university press, ??? (2024)

[19] Rani, P., Sachan, R.K., Kukreja, S.: Bt-cnv: A distributed and decentralized solution for certificate notarization and verification for academia using public blockchain. Peer-to-Peer Networking and Applications **18**(1), 60 (2025)

[20] Wu, J., Lin, K., Lin, D., Zhang, B., Wu, Z., Su, J.: Safeguarding blockchain ecosystem: Understanding and detecting attack transactions on cross-chain bridges. In: Proceedings of the ACM on Web Conference 2025, pp. 4902–4912 (2025)

[21] Wang, S.-W., Tzeng, S.-S., Wang, L.-C.: Slchain: A stochastic lightweight

blockchain with selfish mining attack mitigation. IEEE Internet of Things Journal (2026)

[22] Gupta, N., Naik, V., Sengupta, S.: A firewall for internet of things. In: 2017 9th International Conference on Communication Systems and Networks (COMSNETS), pp. 411–412 (2017). IEEE

[23] Arshad, J., Azad, M.A., Abdeltaif, M.M., Salah, K.: An intrusion detection framework for energy constrained iot devices. Mechanical Systems and Signal Processing **136**, 106436 (2020)

[24] Petrosky, E.E., Michaels, A.J., Ernst, J.M.: A low power iot medium access control for receiver-assigned cdma. International Journal of Interdisciplinary Telecommunications and Networking (IJITN) **11**(2), 24–41 (2019)

[25] Ramadan, R.: Internet of things (iot) security vulnerabilities: A review. PLOMS AI **2**(1) (2022)

[26] Liao, Y., Leung, V.C.M., Gao, S., Huang, Q.: Intrusion detection for the internet of things based on blockchain and trust management. IEEE Transactions on Emerging Topics in Computing **7**(3), 597–611 (2019) https://doi.org/10.1109/TETC.2018.2868663

[27] Yang, K., Blaauw, D., Sylvester, D.: Hardware designs for security in ultra-low-power iot systems: An overview and survey. IEEE Micro **37**(6), 72–89 (2017)

[28] Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Lsb: A lightweight scalable blockchain for iot security and anonymity. Journal of Parallel and Distributed Computing **134**, 180–197 (2019)

[29] Gheisarnejad, M., Khooban, M.H.: Iot-based dc/dc deep learning power converter control: Real-time implementation. IEEE Transactions on Power Electronics **35**(12), 13621–13630 (2020)

[30] Mohamed, N., Oubelaid, A., Almazrouei, S.: Staying ahead of threats: a review of ai and cyber security in power generation and distribution. International Journal of Electrical and Electronics Research **11**(1), 143–147 (2023)

[31] Cui, L., Qu, Y., Xie, G., Zeng, D., Li, R., Shen, S., Yu, S.: Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures. IEEE Transactions on Industrial Informatics **18**(5), 3492–3500 (2021)

[32] Sultana, A., Pabla, T.: The future of mobility: Assessing the impact and applications of blockchain technology in electric vehicle ecosystems. Peer-to-Peer Networking and Applications **18**(5), 263 (2025)