Design of a Zero Trust Security Architecture for Access Control of the Power Internet of Things

Dongmei Bin*, Jieke Lu, Chunyan Yang, Ming Xie, Songming Han

DongMei Bin: bin_dm.sy@gx.csg.cn*, jeke Lu:lu_jk.sy@gx.csg.cn,
ChunYan Yang: yang_cy.sy@gx.csg.cn, Ming Xie: xie_m@gx.csg.cn,
Songming Han: han_sm.sy@gx.csg.cn

(Electric Power Research Institute of Guangxi Power Grid Co., Ltd,Guangxi Nanning,China,530023)

Abstract: In the context of the development of the power of the Internet, this paper will discuss the problems of open communication between IoT electrical terminals, obfuscation of network protection against electrical boundaries, and the difficulty of accessing IoT terminals through traditional security systems. The paper presents a zero-trust architecture as an IoT terminal access security approach, where the IoT terminal itself becomes the source to establish security authentication and control. Respect access. Security authentication of IoT electrical terminals based on fingerprint mining technology and public key generation algorithm for electrical IoT identification has been completed. Perform continuous monitoring of terminal reliability and effective access control with reliable methods based on terminal performance characteristics. In the case of safe access to the distribution of electrical equipment, the corresponding method is used. Embracing a Zero Trust Architecture is a forward-thinking approach to fortifying the security of the Internet of Things against conventional flooding, packet intrusions, and malicious attacks. This innovative access security method ensures timely detection and swift blocking of potential threats, offering a robust defense mechanism against network assaults targeting the power grid terminals within the realm of the Internet of Things.

Keywords: Power Internet of Things; Zero trust; Security architecture

1 Introduction

In the energy industry, the Internet of Things, as well as secondary businesses such as business centers and "generation, network, transport and storage" network management, are developing rapidly, as the network scope expands, node equipment increases, application functions deepen, and data interoperability increases. will have a huge impact on the energy Internet and need to be higher to protect the security network. Contemporary energy grid security strategies prioritize safeguarding its borders. The comprehensive security framework for the secondary network adheres to the principles of 'security zoning, network segmentation, horizontal isolation, and vertical authentication.' This entails a meticulous division between the production control center and the information control unit. Within the production control zone, a further subdivision is implemented, distinguishing between the control zone and the non-control zone, ensuring a nuanced and layered approach to overall security protection. Horizontal isolation devices can be used between network segments, and encryption and authentication devices can be placed on vertical boundaries. Current security uses the principle

PMBDA 2023, December 15-17, Nanjing, People's Republic of China

DOI 10.4108/eai.15-12-2023.2345327

of "one-time authentication and constant trust" in which local network equipment is trusted. As the Internet of Things continues to expand in both power and connectivity, the once well-defined boundaries within large, heterogeneous systems have become more porous and accessible. This evolving landscape poses security challenges, as traditional borders are susceptible to risks and lack comprehensive security analysis and reliability. To address this, a shift in security strategy is imperative, moving beyond the confines of traditional isolation. The transformation involves a reconstruction of the trust management system for personal devices, emphasizing continuous security monitoring. This novel approach advocates for a departure from the conventional notion of trust and embraces the 'zero trust' concept. By implementing security measures that no longer rely solely on borders but extend to constant authentication and access control, the existing secondary electricity systems can be fortified. In the realm of the Internet of Things, adopting zero-trust technology becomes paramount for ensuring security authentication and continuous control over access to IoT terminals. The zero-trust paradigm introduces innovative strategies that comprehensively secure all resource accesses and network requests, providing a robust defense framework to safeguard the power infrastructure of the Internet of Things [1-2].

2 Network security issues faced by the power Internet of Things

2.1 Identity authentication methods need to change

As our company steadily advances in IoT development, connecting millions of terminals, including managed, unmanaged, and user terminals, a new era of requirements has emerged, encompassing large-scale access, heterogeneous authentication, and continuous interaction. In this context, specific challenges related to self-identification have surfaced. Firstly, practical applications often exhibit varying levels of risk and maintenance complexity. To address this, a tiered approach is needed, introducing token recognition technologies with different security levels. This ensures that more frequent and lower-risk applications receive streamlined and efficient authentication, while higher-risk applications benefit from enhanced security measures. Secondly, the intricacies of traditional centralized digital certificate authentication pose challenges for ensuring trust and interoperability within the expansive landscape of the Internet of Things. Hence, there is a need for more flexible and adaptive authentication mechanisms that can accommodate the diverse nature of IoT devices. Thirdly, the development trend of leveraging microservices and applications in the IoT landscape underscores the importance of extending self-identity beyond human users to encompass equipment and services. To achieve this, it becomes crucial to view people, equipment, applications, and services as distinct 'individuals' with their own detailed information. This approach enables the creation of self-management tools tailored to the unique characteristics of each entity, fostering a more comprehensive and effective IoT ecosystem. [3].

2.2 Data security faces new risks

With the introduction of the *Cybersecurity Law*, the country has put forward higher requirements for data security, especially for the protection of critical information infrastructure and important user information. In the application scenario of the Internet of Things in power, a large amount of sensitive data and user information are stored in the cloud, and the entire lifecycle of the data also goes beyond the scope of traditional network security, posing huge security risks. In recent years, incidents of personal information leakage have been frequent and repeatedly prohibited, posing a serious threat to personal life and property security. Once sensitive data is stolen, tampered with, and abused, there is a risk of violating the law. Therefore, it is necessary to strengthen the protection of important enterprise data and customer privacy, and strengthen the establishment of adaptive fine-grained access control authorization for applications, service interfaces, and data.

2.3 Zero Trust Architecture and Solutions

As the Internet of Things (IoT) gains strength, the integration of modern information technologies such as 'Big Cloud IoT Smart Chain' is ushering in a new era of pervasive connectivity and human-machine interaction across various energy sectors. In this dynamic landscape, the once well-defined boundaries of terminal-side networks are becoming increasingly blurred and intricate, rendering traditional security architectures less effective. The power grid, characterized by a multitude of large and fragmented assets, diverse types, and complex environments, poses a unique set of challenges. The ongoing evolution towards document integration in the IoT realm further emphasizes the need for a paradigm shift in security approaches. Adopting a 'zero trust' model can revolutionize traditional security concepts and provide robust support for the intricate dynamics of the 'three-mode, two-network, global level' Internet in the power sector [4-5].

According to the "zero border" of IoT security, self-management is performed to identify IoT devices and services to implement IoT security protection and zero-trust network security architecture. Manage permissions dynamically based on environment and device access characteristics.

2.3.1 Multidimensional Access Control Authorization Policy

Controlling access authorization involves a thorough examination of the various aspects related to the subject, object, and environment in a security assessment. By leveraging data from multiple sources, we gauge potential security risks and trust levels. We establish standardized security quantification criteria and formulate dynamic access control policies. Additionally, a centralized policy center is instituted to guarantee secure and manageable access permissions.

In the interaction scenario of mobile terminals, attribute based dynamic access control strategies are adopted to adaptively grant fine-grained access control authorization to services, applications, and data. Mobile user identity attributes are evaluated based on multi-source data analysis (organizational level security policies and rules, multidimensional attributes of visitors, multidimensional attributes of access targets, environmental attributes, and abnormal behavior evaluation) to obtain access authorization and obtain their trust level. If the trust level evaluated is higher than the minimum trust level required by the access target, authorization is granted.

Traditional security protection is based on the system application itself, resulting in close coupling and lack of elasticity between security protection and system application. It is necessary to establish intermediate layer control and dynamically configure and manage through access policies, which is conducive to flexible business development and dynamic control of security protection. Through trusted proxies, business and application interfaces can be hidden behind trusted proxies and are not visible by default.

The zero trust based authentication and authentication mode further converges the original data acquisition channels of operation and maintenance by standardizing the access paths of devices, users, and services, retaining audits and logs, and ensuring the data security of the system.

2.3.2 Monitoring Audit

By dynamically calculating risks and trust, application access is blocked, allowed and audited, and allowed, continuously monitoring terminal status, and adjusting corresponding access control strategies. Continuously monitor the application's access to the policy center, output access logs to the analysis platform for risk assessment, visualize traffic, use big data analysis and artificial intelligence technology to analyze risks, support risk quantification, and achieve monitoring and auditing of the application's access to the policy center.

Based on big data and artificial intelligence technology, using methods such as traffic collection, behavior pattern learning, security attack monitoring, and security threat response, dynamic perception and intelligent analysis of power IoT security scenarios are achieved, and timely linkage response and disposal of attacks are carried out to ensure the safe and stable operation of the power IoT system[6-7].

3. Zero trust based security framework for the power Internet of Things

3.1 Design of safety protection framework

Establishing trustless security access to IoT terminals based on the nature of IoT in energy. When an entity seeks access to a resource, the initial request is directed to a reliable manager. This manager then conducts a security verification process to assess the identity of the accessing entity. Second, security authentication establishes initial trust, and access control systems grant access to subjects. A bidirectional encrypted data channel is established by a primary access point and an access point that is authorized to transmit data. Resource access is recorded through a dependable manager, and the interaction between entities and resources is implemented within software-defined boundaries. Concealing the actual location of the access device allows the creation of security backups, serving as a preventive measure against unauthorized entities attempting to compromise the capacity of IoT terminals and disrupt the secure functioning of the power grid.

3.2 Safety certification

Securing the access points to the power grid is imperative to safeguard both the terminal and the transmitted data against criminal threats. Additionally, protecting the capacity of the power grid necessitates comprehensive measures to ensure the resilience and integrity of the terminal. Considering the precise communication and low power consumption of IoT terminals connection, the connection points in a large network will increase the complexity of the control system. Risk in security analysis. Therefore, there is a need to study lightweight security authentication systems suitable for IoT terminals.

This paper presents a private public key based security terminal as shown in Figure 1. First, identify the type of IoT flight energy anywhere and eliminate fingerprints; Second, develop an algorithm to generate IoT terminal identification keys based on fingerprints and generate public and private keys for terminal devices; In conclusion, the generation of terminal security authentication relies on the utilization of public key authentication [8].

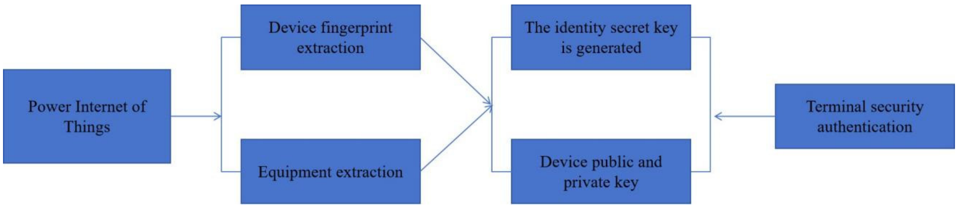
Power Internet of Things
Device fingerprint extraction
Equipment extraction
The identity secret key is generated
Device public and private key
Terminal security authentication

Figure 1 Security authentication method based on identification public key

3.2.1 Device fingerprint extraction

In alignment with the security requirements of the Internet of Things terminal network, we establish the type of terminal management and define a fingerprint feature. This is aimed at sustaining a stable and low-level security posture.

The extraction of fingerprint data goes beyond comprehending device characteristics; it involves identifying the distinct features of certain devices while considering their impact on power and energy consumption. Therefore, as the data contains more content, the mutual information-based multi-label selection algorithm filters out specific content that contains as much information as possible and has a minimum. Terminal fingerprints are shown in Table 1.

Table 1 Fingerprint of Terminal Equipment

Fingerprint features	Describe
Equipment serial number /ID	Unique identifier assigned by the manufacturer to the equipment.
General parameters of equipment	Type, name, model, function, etc.
Embedded module operation condition	Safe state, storage state, etc., with high security and not easy to copy.

3.2.2 Algorithm for generating public key for power IoT identification

The public key generation algorithm for empowering the Internet of Things relies on the Private Public Key (IPK) technology, employing the SM9 algorithm to create key pairs. This evolution of the public key system is progressing towards a comprehensive framework capable of facilitating the identification of IoT devices as well as the authentication of private and public documents. It integrates main signal and distribution to provide basic control of large terminals according to the lightweight basic generation and control method. It will directly simplify and control the complexity of the main characters, while reducing the development and operation of the main system.

The algorithm for generating public keys to enable IoT authentication is as follows.

1) The terminal device captures fingerprint data to create a fingerprint card.

2)The terminal device initiates a process by generating a random number (r) and a pair of public and private keys (r, R) for the user using the SM9 algorithm. It then sends R and the user's ID to the central control center of the device.

3)The device sends R and ID key management hashes to the central control center, resulting in the derivation of 32 sets of mapped locations;

4) Perform parallel operation of 32 layers of sequence plan and generate public and private keys to obtain device pre-key (PSK) and security key (ISK);

5) Subsequently, the key management device employs the encryption algorithm, utilizing R as the public key, to encrypt the ISK. The resulting ciphertext is then sent back to the device.

6)The device, equipped with a corresponding random private key r, decrypts the ciphertext, thereby obtaining the ISK private key.

7)The device control center shares the public PSK, enabling other users to decrypt the ciphertext sent by the device using the device's public key.

3.3 Dynamic Access Control

In a trustless access control system, IoT power components must undergo authentication and authorization each time they establish a connection to the network. This implies that no single security measure can assure the legitimacy of private access. Therefore, during subsequent visits, it is essential to consistently conduct confidence tests, calculate the admission score's confidence level, and employ the admission score as the basis for classification. Best of luck and stay vigilant in the follow-up procedures.

3.3.1 Continuous Trust Assessment

The trust evaluation strategy involves ongoing collection, analysis, and assessment of the network behavior of visiting entities. It dynamically calculates the trust level of these entities. This paper introduces a dependable approach grounded in the operational characteristics of terminals. It delves into the analysis of terminal operational features within the context of Internet of Things capacity, aiming to recognize and establish the reliability of the terminals. The performance characteristics of the terminal are listed in Table 2, including performance, reliability, and security.

Table 2 Terminal operation characteristics

Characteristic	Specific classification
Performance	Processor, memory, disk usage, network traffic information
Reliability	Success rate, packet loss rate, mean time between failures
Security	Number of illegal connections, number of port scans, unauthorized attempts.

When measuring terminal performance characteristics, normal network traffic is defined as normal conditions, and malicious network traffic is defined as uncertain conditions. Network traffic is periodically analyzed to periodically determine whether communications on the current network are secure. The number of normal events is N, and the number of abnormal events is A. Determine whether the network communication is normal as a function of performance, reliability, security, etc. If the number of invalid connections or port scans exceeds the threshold, determine the current network connection. (bf, df, uf}), i.e., calculate the guaranteed TF for the current operation of IoT electrical terminals. Equation (1):(1)

$$\begin{bmatrix} b_{\mathrm{f}} = \dfrac{N}{N+A+1} \\ \mathrm{d}_{\mathrm{f}} = \dfrac{A}{N+A+1} \\ u_f = \dfrac{1}{N+A+1} \end{bmatrix} \tag{1}$$

4 Application Scenario Validation

Based on the evidence, select security conditions for power supply distribution and test various network attacks, such as inverter spoofing to establish connections to data collection servers and data upload terminals. The goal is to define an anti-trust structure for secure access to IoT terminals in the power grid industry [9-10].

4.1 Distributed Power Supply Access Scenarios

Distribution of electrical equipment such as photovoltaic distribution. It is possible to use a transmission network or a wireless network to access the transmission organization, so that the communication center, telephone data and other information can be sent to the main station of the management organization, and remote control, remote control, and remote modification commands can be transmitted. may receive the base station of the management organization. Those. During communication between the power distribution terminal and the power grid, it is imperative to implement security checks and access control measures for the terminal equipment. This is essential to thwart potential attackers seeking to compromise the power supply by tampering with or gaining control of the transmission system to access transmission stations.

4.2 Analysis of Attack Behavior of Distributed Power Supply Terminals

Establishing a test environment for electricity distribution involves the utilization of inverter terminals, data collection servers, and other components. The focus here is on enhancing reliability by integrating robust security measures into IoT terminals. This study leverages the power of the Internet of Things, utilizing public key authentication. It determines power supply distribution and establishes connections between terminals and data collection servers in the power grid. Simultaneously, the paper conducts a trust test for terminals based on their behavior, analyzing simulated attack scenarios like flooding, malicious attacks, and packet attacks. Real-time detection of attack activities is performed, enabling the restriction and blocking of terminal authorizations in response to malicious attacks. Terminal access control, packet parallel control, and settings designed to prevent ship control, avoid attacks, and safeguard network access and power distribution contribute to protecting the power grid from potential damage.

The experimental analysis conducted in this paper provides evidence supporting the efficacy of trustlessness as a robust access method for enhancing IoT security. The approach consistently identifies unusual behaviors in terminals, making effective use of terminal access control mechanisms and consequently lowering the risks associated with network access to the electricity grid originating from terminals.

5 Conclusion

In addressing the security challenges posed by the diverse capabilities of IoT terminals, this paper investigates the concept of trustless security as a framework for IoT terminal access. Recognizing the ubiquitous and varied nature of IoT terminal devices, the paper introduces a lightweight security technology centered around public key identification. Additionally, a dynamic access control method based on terminal parameters is presented, taking into account the potential consequences of network attacks on terminal operations. Experimental findings regarding power availability distribution demonstrate that the proposed method effectively identifies and mitigates malicious activities such as flooding and blocking attacks, thereby reducing risks to the power grid caused by compromised IoT terminals.

Acknowledgement: Science and Technology Project funded by Guangxi Power Grid Corporation (Research and Application Project of Network Trust Support System for New Power System Business Entities (GXKJXM20210257)

References

[1] Chen, Z. , Yan, L. , Zitong Lü, Zhang, Y. , Guo, Y. , & Liu, W. , et al. (2021). Research on zero-trust security protection technology of power iot based on blockchain. Journal of Physics: Conference Series, 1769(1), 012039 (8pp).

[2] Schumacher, S. , & Veeder, H. B. . (2023). The case for print: architecture trade journals as pedagogical tools for disciplinary knowledge. Journal of Documentation, 79(3), 529-545.

[3] Bhattacharjya, S. , & Saiedian, H. . (2022). Establishing and validating secured keys for iot devices: using p3 connection model on a cloud-based architecture. International Journal of Information Security,74(3), 21.

[4] De Oliveira, G. H. C. , Agnaldo, D. S. B. , Nogueira, M. , & Dos Santos, A. L. . (2022). An access control for iot based on network community perception and social trust against sybil attacks. International journal of network management,76(1), 32.

[5] Han, C. , Kim, G. J. , Alfarraj, O. , Tolba, A. , & Ren, Y. . (2022). Zt-bds: a secure blockchain-based zero-trust data storage scheme in 6g edge iot. Journal of Internet Technology,36(2), 23.

[6] Kumar, R. A. , & Vinuthna, K. . (2021). Randomized ensemble svm based deep learning with verifiable dynamic access control using user revocation in iot architecture. Sadhana: Academy

Proceedings in Engineering Science,54(4), 46.

[7] Rane, S. B. , & Narvel, Y. A. M. . (2021). Re-designing the business organization using disruptive innovations based on blockchain-iot integrated architecture for improving agility in future industry 4.0. Benchmarking,21(5), 28.

[8] Jin, Q. , & Wang, L. . (2021). Zero-trust based distributed collaborative dynamic access control scheme with deep multi-agent reinforcement learning. Security and Safety, 8(27), 170246.

[9] Agyekum, M. P. , Odopey, S. A. , Asiamah, S. , Wallis, L. , Williams, J. E. O. , & Locke, R. . (2023). "improved access, delayed accreditation, low recognition": perspectives of mental health educators, preceptors and students on the kintampo project in ghana. The Journal of Mental Health Training, Education and Practice, 18(4), 277-287.

[10] Nazim, M. , & Ashar, M. . (2023). Factors influencing the adoption and use of open access scholarly communication among researchers in india. Online Information Review, 47(2), 259-282.