Retraction

Retraction: Access Point Authentication Scheme of SCADA System Based on Cloud Computing Technology (J. Phys.: Conf. Ser. 1748 022010)

Published 9 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction.

Retraction published: 9 September 2022

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Published under licence by IOP Publishing Ltd
Access Point Authentication Scheme of SCADA System Based on Cloud Computing Technology

Jiayuan Shen*, Jun Xu1, Kun Cai1 and Yan Ji2
1 Zhejiang Zheneng Natural Gas Operation Co., Ltd., Hangzhou, Zhejiang, 310052, China
2 Zhejiang Provincial Energy Group Company Ltd., Hangzhou, Zhejiang, 330110, China
* Corresponding author’s e-mail: shenjiayuan@zjenergy.com.cn

Abstract. Aiming at the security problem of the SCADA system introduced into cloud computing that lacks a credible identity authentication mechanism, this paper proposes a cloud computing-based SCADA system access point authentication scheme. In this scheme, a cloud service security access protocol for SCADA system is proposed. The protocol uses password based identity authentication technology to screen the identity of the terminal node, and effectively identifies the illegal access point by authenticating the access point. By this method, the user’s private information is prevented from being intercepted and tampered maliciously.

1. Introduction
The main components of SCADA (Supervisory Control And Data Acquisition) system include Remote Terminal Unit, monitoring computer, Programmable Logic Controllers, communication infrastructure and Human Machine Interface, etc. [1], can be used to collect and monitor data in many fields such as electricity, water supply, logistics and transportation, and process control.

In order to cope with the big data computing performance challenges faced by SCADA systems, reference [2] introduced cloud computing into SCADA systems. Cloud computing has the characteristics of distributed computing and can store data in the cloud, which makes cloud computing-based applications have flexible scalability and easy management characteristics. The introduction of cloud computing into the SCADA system can effectively solve the performance problems caused by big data. However, the SCADA system based on cloud computing still has the security flaw of lack of a trusted identity authentication mechanism [3].

The security of the network depends on the weakest link in the entire security chain. The connection point with the industrial control system environment can be accessed by multiple equipment and system suppliers, and the security is low. With the rapid increase in the number of access points and the lack of effective authentication mechanisms, companies cannot judge whether the personnel who establish and manage connections through these access points are safe [4]. With the increase in the number of devices connected to the industrial Internet of things, this problem will only become more prominent. The new access terminal may bring a variety of security risks to the whole system, such as illegal occupation of enterprise network and resources, full of virus Trojans, disclosure of enterprise secrets, illegal access and personnel intrusion through the new terminal [5]. Therefore, in order to ensure that the hardware, software and information of the SCADA system will not be destroyed by natural and man-made factors, we must first solve the network security problems caused
by the access of the terminal [6].

In reference [6], the method of unique matching between physical equipment and address is used, and the firewall access rules are set up to set the program access port through the firewall to realize the filtering of the program and the security authentication of the intranet access terminal. Reference [7] proposes to use Trustzone security extension technology to build a highly trusted mobile terminal system, so as to achieve secure access, and experiments show that the scheme is efficient, flexible and easy to expand. Reference [8] proposed a system security access technology based on identity authentication for wind farm SCADA, described the system framework and structure design, and built a security access control model to realize the safe and smooth operation of wind farm SCADA system.

In reference [9], aiming at the problems of data tampering and data leakage in the micro grid SCADA system in remote areas, a self-authentication identity authentication protocol is proposed. In addition, the protocol can reduce the traffic and reduce the communication cost, which is more suitable for the application scenarios of "remote areas". According to the special demand of "civil air defense" in the power Internet of things, reference [10] proposes to build a cloud service platform to achieve trusted identity authentication, so that it can provide a trusted identity database including the Internet and the national network information network.

In view of this situation, this paper proposes an access point protection scheme of SCADA system based on cloud computing, which can realize secure access when the equipment terminal is connected to the cloud and SCADA system, verify the connection's identity, ensure the legitimacy of the terminal before allowing the terminal to access the communication server, so that its access behavior is regulated.

2. Access Point Authentication Scheme

How to avoid the attack risk caused by the introduction of new terminals has become a problem that must be solved. In view of this, this paper proposes an access point authentication scheme of SCADA system based on cloud computing, which ensures that only legitimate and trusted user terminals can enter the SCADA system to obtain data and information through access point authentication. This paper intends to use cloud service security protocol to realize the identity identification of access point.

Cloud-based SCADA systems collect and display data from PLC or RTU, which is essentially an one-way communication and provides status information within the facility. There are many access points in the system, including remote workers, control systems, third-party suppliers, subcontractors, contractors and customers, etc., which are prone to multiple vulnerabilities when facilities are connected to multiple access points. The main access point needs to upgrade, monitor, repair or access the system to obtain remote connection permissions, such as accessing data through wireless local area network, or using facilities such as personal computers, personal digital assistants and modems to remotely access SCADA systems.

![SCADA architecture based on cloud computing](image_url)

Figure 1. SCADA architecture based on cloud computing

If users want to enter the network to obtain or transmit information, they must first verify the security of the access point and set the access point as the first line of protection. The participating
entities of the cloud service security access protocol are users such as PC, PDA and Modem, control system and third-party providers. The process of protocol implementation is shown in figure 2.

![Sequence Diagram](image)

Figure 2. Sequence diagram of secure access protocol

1) when the user (U) needs to access the data in the system, it needs to initiate an access request to the third-party provider (T). The user sends an access request to the user, which includes the unique identification (device_ID) of the user's ID (UID), device, the local certificate issuance timestamp (TP), and the digital identity certificate (DIC). These messages are combined to form an authentication request message:

\[ U \rightarrow T: \text{sigCK}_{\text{pri}}(\text{UID}, \text{device_ID}, \text{Tkpub}, \text{TP}, \text{DIC}) \]

\[ T \rightarrow U: \text{sigTK}_{\text{pri}}(\text{nonceT}, \text{TKpub}) \]

Where \( \text{sigCK}_{\text{pri}}() \) means to sign with the private key of the identity key of the device; \( \text{Tkpub} \) means that the public key provided by the third-party vendor; \( \text{sigTK}_{\text{pri}}() \) means that it is signed with the identification key provided by the third party.

There are a variety of devices connected to the cloud-based SCADA system, and a unique identifier based on attribute characteristics can be set for each device, which can be used as the basis for device access and identity authentication for matching verification, and cooperate with password-based authentication methods to verify the legitimacy of the access point.

Because mobile devices and remote terminals are mobile and need to reestablish connections frequently, in order to further enhance secure access, add a timestamp to the admission authorization certificate as a fresh factor and set the certificate survival time, so that the authorization certificate is timely and effectively prevent the risk of replay attacks caused by frequent terminal replacement.

2) The third-party supplier sends access authorization to the third-party supplier after passing the legitimacy certification. The user needs to verify the time stamp of the certificate when applying for access. If the time difference between the time stamp and the current time is within the specified period, if it is not satisfied, the verification will fail, the access will be invalid, and no result will be returned. If it is satisfied, the verification will continue.

3) After the completion of verification, the third-party supplier will send the authenticated user information to the control system (C), and the control system will recognize the legitimacy of this user.

The access point obtains the value of the unique identifier of the device, uses the device's identity certification private key to sign the random number and device_ID generated by the third-party provider, and obtains the message \( = \text{sigCK}_{\text{pri}}(\text{UID}, \text{nonceT}) \), and the third-party provider uses the public key to transfer massage. After being encrypted with the key certificate, the information is sent to the control system.

4) At this time, the user can carry the authentication certificate to initiate an access request to the control system.

5) The control system confirms the certificate again and returns the verification result.

6) Users can smoothly access the SCADA system for normal data interaction, and upgrade, monitor, repair or access the data in the SCADA system according to their own authority and
responsibilities.

There is no need to consider the security of the communication channel between the user and the server and the security of the server itself in the cloud environment, this article uses the cloud service secure access protocol, which can resist malicious server attacks. Realize convenient and reliable access point identity authentication. Through identity authentication, prevent users from malicious interception and tampering, and prevent the disclosure of private information during user identity confirmation, thereby shielding illegal intrusions or attacks; granting permissions to safe users.

In addition, set up firewall access rules for LAN users. Establish a security gateway erected between the external and internal networks to protect the internal network and prevent the intrusion of illegal programs. The program needs to access the network through a specific port. If the port corresponding to the program is blocked, it can be prevented from running. Use firewall software to track the records, record the port numbers through which the data passes during each visit, and summarize the range of port numbers for SCADA access programs. Define firewall access control rules to allow legitimate users to access and filter out illegal users.

3. Performance analysis

3.1. Security analysis

In reference [6], the device and filtering are carried out through the firewall, the operating system is simplified, the physical input device is shielded, a unique number is set for the legitimate visitor terminal in the intranet, and recorded in the firewall together with the physical address. In reference [7], Trustzone technology is used to build a trusted mobile terminal architecture, but the anonymity of application service providers and cloud service providers is not taken into account. Reference [9] uses a recoverable message signature scheme to create a protocol design with message recovery. It has been proved that this method can effectively achieve data secrecy, effectively resist attacks such as replay, forgery and tampering, and has more efficient operation efficiency. Reference [10] designs a secure access control model for the system database, which designs a credibility calculation module, and creates an identity authentication module on the basis of PKI. Through identity authentication and credibility calculation, secure access to the wind farm system is realized to ensure the security of data transmission. As can be seen from Table 1, the scheme in this paper has the dual protection of network and physical equipment, anonymity and good applicability at the same time.

| Scheme                | Equipment Protection | Network Protection | Anonymity | Applicability | Duration of Authorization | Tampering |
|-----------------------|----------------------|---------------------|-----------|---------------|--------------------------|-----------|
| reference [6]         | √                    | --                  | --        | ×             | --                       | --        |
| reference [7]         | --                   | √                   | ×         | √             | --                       | √         |
| reference [9]         | --                   | √                   | √         | ×             | --                       | √         |
| reference [10]        | --                   | --                  | --        | --            | --                       | --        |
| The proposed scheme   | √                    | √                   | √         | √             | √                        | √         |
3.2. Performance analysis

The system designed in this paper is compared with the trusted mobile terminal system constructed by trustzone technology proposed in reference [7] and the secure access protocol mentioned in reference [9]. According to the local software and hardware environment, the same experimental operation is carried out, and the average delay time of user access request in 100 experiments is taken as the reference result, and because the authorization has a certain period of validity, the system designed in this paper is compared with the trusted mobile terminal system constructed by trustzone technology and the secure access protocol mentioned in reference [9]. Users do not have to apply for permission multiple times during a trial, so they have a certain tolerance for delay. Figure 3 shows that the protocol proposed in this paper can effectively reduce the delay time when multiple users initiate requests at the same time.

4. Conclusion

This paper proposes an access point authentication scheme for cloud-based SCADA systems, which uses password-based methods to authenticate user legitimacy and grant permissions. The cloud service security access protocol is used to identify the newly added remote access points of the SCADA system. Firewall access rules are set up to protect the access points within the LAN.

Reference

[1] Zheng S, Xu W, Shi B. Current Status of Safety in Industrial Control Systems [J]. Network Security Technology and Applications , 2020(05): 111-113.
[2] Wan Y. SCADA System Design Based on Cloud Computing Technology[J]. High Voltage Apparatus, 2013, 49(07): 89-91+95.
[3] Liu C, Zhou L. Network Security Technology Implementation in Big Data Cloud Computing[J]. Computer knowledge and Technology, 14(19): 28-29.
[4] Rusty Gavin. Cybersecurity for cloud-based SCADA. 2018, 65(8): 50-52.
[5] Xiong S. Path of Network Security Technology Implementation under Big Data Cloud Computing[J]. Electronic testing, 2018(08): 79-80+126.
[6] Cai Y. Discussion on Safety Protection of ACCESS Terminal of SCADA System in Yellow River Diversion Protection[J]. Mechanical Engineering and Automation, 2020(04): 212-213.
[7] Yang B, Feng D, Qin Y, Zhang Y. Secure Access Scheme of Cloud Services for Trusted Mobile Terminals using TrustZone[J]. Journal of Software, 2016, 27(06): 1366-1383.
[8] Liang T, Li Y, Xu Y, Yang J. Design of Cloud Platform Based on Wind Farm SCADA System[J]. China Testing, 2019, 45(10): 114-119.
[9] Zuo L, Zhang M, Ding S, Chen Y. Identity Authentication Protocol With Message Recovery in Microgrid SCADA System [J]. Grid Technology, 2019, 43(12): 4299-4306.
[10] Feng L. Secure Access Technology of Wind Farm SCADA System Based on Identity Authentication[J]. Electronic Technology and Software Engineering, 2020(02): 256-258.

[11] Wu Z. Implementation of Network Security Technology in Big Data Cloud Computing[J]. Electronic Technology and Software Engineering, 2020(12): 259-260.