Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 1578-1584
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

# Research and Practice of Cloud Application Security Based on Multi Factor Authentication Technology

**Qianru Gong**[*]
Electronic Information Engineering College, Henan Polytechnic Institute, Nanyang, Henan, China
*Corresponding Author.

***Abstract:***

Identity authentication is one of the key mechanisms to ensure Cyberspace Security. Single factor authentication method has the shortcomings of easy to be attacked and weak security. The use of multi factor authentication including user biometrics has become the main way at present. Aiming at the problems faced by multi factor authentication scheme in different application environments, aiming at increasing the security and operation efficiency of the scheme, this paper studies the multi factor remote authentication method combined with zero knowledge proof technology. This paper proposes the concept of zero knowledge token, and designs and implements it based on elliptic curve and hash function. Compared with other existing solutions, this solution has better availability, scalability and security. The comparison results show that this scheme has lower communication overhead than other existing schemes. Under the condition of maintaining the same level of computing time overhead, the security of the identity authentication process is enhanced..

***Keywords***: *Identity Authentication, Multi Factor, Zero Knowledge Token, Hash Function..*

## I. INTRODUCTION

Since the late 1990s, grid computing has been regarded as an important research direction. However, so far, the grid has not achieved the expected prosperity. In order to meet the needs of today's massive information search and use, it giant Google has designed a new "super server" computing architecture, which has strong scalability, and then this architecture is called cloud computing system [1-2]. However, there is no doubt that cloud computing is still in its early stage of development, many of its technologies are still immature, and there are still many problems to be solved. As early as 2008, Frank gens, senior vice president and principal analyst of IDC, an international data company, pointed out nine challenges and problems faced by cloud computing services in his analysis report. In order to solve such cloud computing security problems, this topic first discusses in detail the main problems faced by cloud computing at this stage, and then studies and discusses the solutions to these problems by using existing security technologies [3-7]. The research of this topic has important reference value for ensuring the security of cloud computing system, improving the efficiency of cloud computing and promoting the development of cloud computing.

## II. CLOUD COMPUTING INFRASTRUCTURE SECURITY

### 2.1 Cloud computing network layer security

When analyzing the security of cloud computing framework from the network layer, it is necessary to distinguish between public cloud and private cloud, because there will be new attacks, vulnerabilities and changes in information security topology risks specific to individuals [8]. Although the common network topology changes little, the choice of private network may not change. When we use an extranet (for example, for large customers or strategic partners), there may already be a network topology suitable for private cloud in use.

Nowadays, more and more data or institutional personnel rely on external host devices to ensure the availability of cloud service resources, and are more and more lazy about network layer security. The three risk factors listed earlier are also included in this risk range. BGP prefix hijacking is a good example of such risk factors. Prefix hijacking refers to that a BGP router illegally declares the IP address space (or prefix) of other network operators, but does not actually forward IP packets with the target address in the prefix. Illegal intrusion or misconfiguration of BGP router are easy to form prefix hijacking attack. Incorrect configuration will not only cause prefix hijacking, but also affect the availability of cloud resources. According to a research report submitted by the North American network operations organization (Nanog) in February 2006, hundreds of such misconfigurations occur every month [9-10].

In addition to misconfiguration, prefix hijacking caused by deliberate attacks is rare, but it still occurs and can prevent access to data. According to Nanog's research report, such attacks are less than 100 times a month. Although prefix hijacking has appeared for a long time, such attacks threaten cloud computing to a great extent. With the increasing use of cloud computing, the availability of cloud resources is becoming more and more valuable to users, which also increases the risk of malicious behavior affecting its availability.

### 2.2 Application layer security analysis

According to sans, vulnerabilities in open resource websites and user based applications accounted for more than half of the total number of vulnerabilities found from November 2006 to October 2007. Many hackers took advantage of some well-known vulnerabilities (such as OWASP TOP10) to carry out cross site scripting attacks (XSS), SQL injection, execution of bad habit programs, etc. Hackers constantly scan websites to find loopholes, and then use these loopholes to engage in illegal acts, such as financial fraud, theft of intellectual property rights, phishing, transforming trusted websites into malicious servers using client services, etc. All website frameworks and all forms of website applications have their security defects, such as incomplete authentication, application logic errors, etc. a website application established and deployed on the public cloud platform should also withstand the test of viruses and Trojans, and may be used by hackers to engage in fraud and other illegal activities.

Under this threat, the website application (SPI mode) deployed in the public cloud must be able to effectively resist these threats from the Internet, so the design of security must also be included in the software life cycle. In the public cloud, the support of service providers for user security is limited, such as application firewall, SSL accelerator, encryption and PKCs 12 device management. It is not supported by public SaaS, IAAs and PAAS clouds. IAAs and PAAS service providers may provide some complex security policies in the future, but now all controls that need to configure applications or connect peripherals locally are unavailable. In the private cloud, we can use a combination of peripheral security controls deployed in a secure environment and network-based and host based access control to protect website applications (including internal network and private cloud) and resist external hacker attacks.

DDoS attacks on the cloud and application layer can prolong the time of DDoS attacks. These attacks usually come from zombie computer systems connected to the Internet (hackers hijack, control computers infected by viruses, worms, malware or unprotected large servers). The DoS attack at the application layer is represented by a large number of web pages reloading XML website service requests (through HTTP or ht'tps) or specific protocol requests supported by ECs. When such malicious requests are mixed into legitimate traffic, it becomes very difficult to filter out these malicious traffic without affecting the integrity of the server.

In addition to bringing trouble and bad service impression to users, DoS attacks on pay as you go cloud applications will greatly increase the cost of cloud services. At the same time, users will also feel the increase of network broadband, CPU and storage usage. This type of attack is also described as denial of economic sustainability (EDOS).

## III. SECURITY ANALYSIS OF CLOUD STORAGE

### 3.1 Credibility

When discussing the credibility of data stored in the public cloud, we should first decide what kind of access control to protect data. Access control includes authorization and authentication. Service providers usually use weak authentication mechanisms (such as user name and password), and the authorized access control that users can use is often very rough. In view of this defect, this paper designs a new security authentication mechanism, which will be discussed in Chapter 8.

Secondly, encryption should be used to protect the data in the cloud. However, due to cost considerations, different service chambers adopt different encryption strategies. For example, EMC's mozyenterprise provides data encryption services to users, but AWS S3 is different. Users can encrypt data themselves before uploading, while S3 itself does not provide encryption services.

Different service providers will also choose different encryption algorithms and key strength. Not all encryption algorithms can guarantee the security of data. Only algorithms that have been authorized (such as NIST) or at least reviewed by the encryption community can be used. Encryption can be divided into symmetric encryption and asymmetric encryption. When the encryption key and decryption key are the same, we call the encryption algorithm symmetric encryption, and vice versa.

The last encryption credibility problem is key management. Key management is complex and difficult for individual users, even for service providers. Many service providers use the same key to encrypt data for all users. Therefore, for users, the cloud service provider should not be allowed to manage the key as far as possible, at least not the service provider for data storage. In order to prevent the key from being damaged or lost, we can use key escrow encryption technology.

### 3.2 Usability

When a user's data has been protected by credibility and integrity, its availability becomes particularly important. There are two main threats in this regard. The first is cyber attack, which we have discussed in Section 1 of Chapter 3 and will skip here. The second is the availability of service provider facilities. No service provider can guarantee that its facilities will always be in normal operation. Table 1 shows the report on the abnormal operation time of cloud service providers' facilities in the United States.

**TABLE I. Average abnormal operation time of cloud service provider facilities in the United States**

| | **Downtime (Hours: Minutes: Seconds)** | | |
|---|---|---|---|
| Usability | Every day | Monthly | Annually |
| 99. 9999% | 00:00.4 | 0:00:26 | 0:05:15 |
| 99. 99% | 0:00:08 | 0:04:22 | 0:52:35 |
| 99. 9% | 0:01:26 | 0:43:49 | 8:45:56 |
| 99% | 0:14:23 | 7:18:17 | 87:39:29 |

No matter how complete the equipment of service providers is, service interruption is always unavoidable. For example, Amazon S3 was interrupted for two and a half hours in February 2008 and eight hours in July 2008. AWS is already a cloud service provider with mature technology, so you can imagine how long the service will be interrupted when a small or less mature cloud service provider encounters unpredictable problems such as power failure. From table 1, we can see that 99.9999% of cloud service providers have more than five minutes of service downtime every year, but for 99% of manufacturers, this figure reaches as much as 87 hours.

## IV. AUTHENTICATION AND ACCESS MANAGEMENT

### 4.1 Trusted surroundings and Iam

In an enterprise, the surrounding environment of trusted applications is mostly static and monitored and controlled by the IT department. When cloud services are adopted, the trusted boundary of the enterprise will become dynamic and beyond the control of the IT department. At this time, the boundaries of networks, systems and applications in enterprises will be extended to the field of service providers, which challenges the trust between enterprises and service providers. Many traditional enterprises take a wait-and-see attitude towards cloud computing due to the fear of the leakage of internal sensitive information, which hinders the development of cloud computing to a certain extent.

For enterprises using cloud computing services, in order to strengthen their ability to control resources and resist risks, enterprises will be forced to use other high-level controls, such as application security and user access controls. The centralized authentication and authorization of the enterprise's website will greatly accelerate the use of Iam services.

However, 1am within an enterprise may lack a core management and identity information framework. Generally, identity storage is managed manually by multi tenant administrators, and the application processes provided to users will not be well deployed. These processes are not only inefficient, but also often make mistakes. For service providers, they need to support Iam standards (such as SAML), use user alliances to expand their services and comply with Internet standards and regulations. Cloud services supporting Iam will accelerate the migration of traditional IT applications from trusted networks within enterprises to trusted cloud services. For users, perfect IAM process and cloud services supporting SAML IAM standards can effectively protect the credibility, integrity and management agreement of information stored in the cloud.

### 4.2 IAM analysis in cloud

In today's IAM technology stage, the standards supported by service providers (IaaS, PaaS, SaaS) are not perfect. Although large service providers, such as Google, Microsoft and Saleforce.com, have demonstrated their basic IAM capabilities, they still lack the requirements of enterprises for monitoring management, privacy and data protection. Table 2 illustrates the comparison of SPI mature models in IAM.

The mature model takes into account the dynamic environment of IAM users, systems and cloud applications, and solves four key components in the IAM automation process: user management and new users, user management and user modification, authentication management and authorization management.

**TABLE 2. Comparison of SPI mature models in IAM**

| | SaaS | PaaS | IaaS |
|---|---|---|---|
| User management, new user | Available | Immature | Mature theory |
| User management, user modification | Available | Immature | Immature |
| Authentication management | Available | Mature theory | Available |
| Authorization management | Mature theory | Immature | Immature |

Although the established enterprise Iam can be applied to cloud services in principle, they still need to be adjusted to adapt to the cloud environment. Generally, user management in the cloud can be summarized in the following aspects.

Cloud identity management function should focus on cloud user identity life cycle management: distribution, recycling, identity alliance, sso, password or certificate management, personal data management, management authority management, etc. Enterprises that do not support identity alliance should explore cloud based identity management services. This new service usually synchronizes its directory (usually multi-user) with the internal directory of the enterprise and acts as a proxy for the enterprise IdP.

Medium and large enterprises usually have special needs for the authorization function of their cloud users. In some cases, an enterprise application may need role-based access control (RBAC). In this case, authorization needs to meet the functional role requirements of the enterprise. At present, the authorization and management of cloud services are not perfect and may not meet the needs of enterprises. Most cloud services support at least dual roles (permissions): administrator and end user. It is also normal to provide administrator permissions in service providers. These permissions allow administrators to assign and reclaim permissions, identity attributes, and set access control policies (such as enhancing passwords and trusting networks that accept connections). XACML is a popular compulsory authorization and user authorization standard.

## V. CONCLUSION

With the rapid development of the network, the explosive rise of network data traffic, the straight-line rise of the cost of traditional network storage center, and the demand for high-speed computing, now it has transitioned from the era of equipment to the era of network. This gives the necessary conditions for the emergence and development of cloud computing system composed of a series of interrelated and virtualized computers. The necessary conditions for the emergence and development of unification. However, the lack of standards and immature technology pose considerable security risks to cloud computing. This paper discusses the security risks of cloud computing authentication, data, storage, application, virtual technology, access, security patch and post response from IAAs, SaaS and PAAS frameworks, and puts forward corresponding solutions. The security responsibilities of cloud framework are analyzed from the perspective of service providers and users.

## ACKNOWLEDGEMENTS

This project was supported by the sub-project of the Young Backbone Teacher Training Program of Henan Province Colleges and Universities (Grant No. 2016GGJS-236).

*Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022*

## REFERENCES

[1] Liu Jian Research on secure government network based on trusted virtualization technology. Industrial design, 2017 (7): 3

[2] Shao Xiaohui, Ji Yuanxiang, Le Huan Research and practice of omni-directional and multi angle information security technology in cloud computing and big data environment. Science and Technology Bulletin, 2017

[3] Zhou Junping, Fu Wei, Zhang Lei, et al Research on the application of cloud authentication security technology in the field of international trade. Information security and communication confidentiality, 2012 (11): 4

[4] Wu Weiqiang Research and practice of omni-directional and multi angle information security technology in cloud computing and big data environment. Communication world, 2017 (14): 2

[5] Zhou que, Zhou Yu, Zhang Nian Research and practice of omni-directional and multi angle information security technology in cloud computing and big data environment. Digital users, 2019 (11)

[6] Li Jun Research and practice of information security technology in cloud computing environment. China new communications, 2019 (14): 1

[7] Wu Shaoying Research and practice of information security technology in the context of cloud computing and big data. Computer fan, 2018 (9): 1

[8] Yue Jianbin Application of dynamic two factor security authentication technology based on MD5 algorithm in enterprise ERP system. Automation and instrumentation, 2010 (06): 84-85

[9] Li Peng Research on fingerprint authentication technology for security and privacy. Graduate, 2011

[10] Xu Xiao Application analysis of USBKEY identity authentication system. Online education, 2011, 000 (006): 95-96