Unified Identity Authentication Design of Various IoT and Cloud Computing Based Information Systems Integration

Xiaodong Wang*, Xiquan Dong, Cheng Zhong, Yan Liu, Peng Chen

Beijing Aerospace Control Center, Beijing, China

*Corresponding author: sjtuwxd@163.com

Keywords: Unified Authentication, Identity, Account, Security, Information Systems, IoT and Cloud Computing.

Abstract: The era of information and big data changes the way people live, work and think. Many Information systems are integrated together to fulfill various management and service purposes in a specific zone like a campus. But along with different systems, the question of insecurity, inconvenience, and inconsistence in identity authentication arise. We are faced with the same question when building and integrating different systems of security protection, personnel and car management, electric power and energy systems monitoring based on internet of things, cloud computing. To solve this, a unified identity authentication management system is proposed, designed and fulfilled. In the system, issues of unified identity authentication, account management, access authorization, access audit, security management and Single sign-on are well considered and handled. Among identity authentication mode, USB key, soft certificate, LDAP authentication mode, AD domain, dynamic and static password, shared authentication and radius authentication methods are designed to satisfy different authentication needs of various applications underneath. Besides, the unified identity authentication management system provides an authentication interface. The newly developed application system can integrate with it by calling the authentication interface. The characteristics of application independence, high Security and reliability, scalability, cross-platform feature is included in system accomplishing.

1. The Introduction of Background

In the face of the below problems, security measures should be taken to ensure the security of system access and management, rather than only meet the functions provided by the application system.

Identity authentication issue: Nowadays, most authentication methods of each application system are through username and static password login systems. However, the static password has significant security risks, including easy to intercept and analyze, even guessing and cracking. The probability of leakage is substantial. Once others use the password, they can access the application system without authorization; others can illegally obtain confidential information. Some accounts and passwords are even used by groups of people. In a security accident, it is difficult to determine the responsibility and challenging to control the spread of accounts at ordinary times. It will be easy to cause varieties of security flaws [1, 2].

Account management issue: The number of application systems and devices is increasing dramatically. Each application system and device are independent and have its own account management modules; these accounts can easily confuse account management. System management has great security risks since they are independent [3].

Access control issue: Each application system lacks a unified access control entrance, and each system independently opens its address and port to provide access [4]. The system administrator can directly add or delete users on each system and authorize them. With the increase of the system, there will undoubtedly be more ways for illegal personnel to enter the system.

System login issue: With the increasing number of application systems, users are often required to switch between different systems. Users need to enter usernames and passwords frequently to log in. It inconveniences users and affects working efficiency [5]. Some people set the same password for multiple systems—it endangers the security of the application system.

Security management: Each application system maintains an authentication, authorization, and audit system independently and is managed and maintained by the corresponding administrator. As the number of systems increases, the complexity of the system administrator's work increases exponentially, especially spending countless time adding and deleting users and changing passwords [6]. Sometimes, forgetting to remove a former employee from the system creates a significant security risk.

2. Unified Identity Authentication Management System

Given the above considerations in the introduction, we fulfilled the following features in our unified identity authentication management system.

Unified identity authentication: The internal user can be authenticated in various ways to provide strong identity authentication and provide identity authentication services for application systems, including digital certificates, dynamic passwords, LDAP authentication, and Radius authentication [7]. It’s important to provide a unified identity authentication source and establish a centralized identity management platform.

Unified account management: Unified account management of the same application system is implemented on the Unified Identity Authentication Management system to avoid decentralized account management, resulting in illegal accounts.

Unified access authorization: The Unified Identity Authentication Management system protects all application systems in the integrated system and authorizes each user according to different security strategies. The specific system's access of each user will be determined accordingly. Role-based authorization management is implemented for applications. When personnel leaves or changes positions, the user's access permission can be changed by applying modification on the platform. It will eliminate security risks caused by self-authorization or expired authorization.

Unified access audit: Uniformly record the activities of each user login in each system and ensure complete records, reliably record the use process of managers and end-users to establish comprehensive and practical backtracking and tracing mechanism. Make statistical analysis on the access status of all systems to clearly understand the access status of the system and detect illegal access behaviors in advance.

Unified security management: Manage users' accounts, identity authentication methods, and permissions in a unified manner on the platform. Manage application systems and audit information in a unified manner. Implement a unified security policy internally.

Single sign-on (SSO): After a single login, all authorized systems can be accessed without re-entering the account and password of the original system.

3. Identity Authentication Mode

The Unified Identity Authentication Management system supports digital certificate authentication, dynamic password authentication, and static password authentication. For digital certificates, the Unified Identity Authentication Management system supports soft certificate authentication and USB Key authentication to meet different security requirements of enterprises. In addition, interfaces are reserved to support the third-party strong authentication protocol.

The digital certificate is a series of data containing the identity information of network users. It is used to identify each other in the network communication, that is, to solve the problem of "who I am" on the Internet. Like in reality, each of us should have a proof of personal identity card to show our identity. A digital certificate usually contains a unique name. This name uniquely identifies the certificate issuer, the certificate owner's public key, the digital signature of the certificate issuer, the validity period of the certificate, and the certificate's serial number.

It is based on the public key (asymmetric encryption and decryption technology) to encrypt and decrypt the information transmitted on the network and performs digital signature and signature verification. It can ensure the confidentiality and integrity of the data transmitted online. It also can guarantee the identity authentication of the operating entity and the non-repudiation of the signature information to ensure the security of network applications.

3.1 USB Key

As an effective method to confirm users' identities and protect users' data, digital certificates have been accepted by more people. A USB Key that stores encrypted information is the best carrier of a digital certificate. The USB Key is capable of storing private information and generating public and private Key pairs of certificates. It also protects the private key from being held in the key. Moreover, the private key is capable of providing encryption operations to support certificate signing and authentication operations.

A USB Key is an electronic device. A PIN code is required to use the certificate Key. The security of certificates can be ensured by USB Key hardware and PIN protection for keys.

As long as the USB Key is inserted into the personal terminal, the application system will automatically read the user's identification and log in to the corresponding application system, just like opening the door with a Key. Without the USB key or unauthorized users will not be able to enter the system. After the USB key is removed, the system will lock immediately. Only after the USB Key is inserted again, the user can use the unified identity management system again to access internal resources in the integrated system.

3.2 Soft Certificate

Digital certificates are stored as disk files, either on a local machine, a floppy disk, or a USB flash drive. This storage mode only protects the certificate with a PIN code but does not encrypt and prevent copy control. This method is only applicable to users who require low-security levels or the application system that doesn't require a high level of confidential data or permissions. For example, the current online tax declaration system often uses this digital certificate storage mode.

3.3 LDAP Authentication Mode

The Unified Identity Authentication Management system provides multiple built-in authentication modes. LDAP is the default authentication mode provided by the unified identity management system. In LDAP authentication mode, the username and password are stored in a specified LDAP directory. When a user logs in, if the username and password provided by the user match with those recorded in the stator tree of the LDAP directory, the authentication succeeds. The user has the identity corresponding to the user record in the LDAP directory.

3.4 The AD Domain Authentication

If an AD domain exists in the integrated system, the Unified Identity Authentication Management system can use the domain authentication system as its authentication mechanism. If a user passes the AD domain authentication, the user passes the authentication.

3.5 Dynamic Password Authentication

Dynamic password technology is commonly used to control access to essential resources such as hosts and servers. It can also be used to control access to some special users, such as privileged users of the system. The Unified Identity Authentication Management system platform can use the third-party dynamic password authentication system and combine it with the third-party dynamic password authentication server. Dynamic password authentication is implemented. Dynamic password card is a mature method, and it has been successfully used for many years around the globe.

3.6 Static Password Authentication

Static password authentication is the most basic and traditional convenient authentication mode. The Unified Identity Authentication Management system still maintains this authentication mode to facilitate the authentication selection of users. Users who do not require a high level of information confidentiality can use this mode. The static password security strategy of the Unified Identity Authentication Management system can set complex password requirements, such as digits, alphanumeric combinations, etc. Even validation period.

3.7 Shared Authentication

Unified Identity Authentication management system allows the administrator to set multiple users to share the same account and password. In such a way, if a branch office, branch organization, or department has the same permission but does not want to remember multiple usernames and passwords, it can assign a unified account and password to implement shared authentication on system access.

3.8 The Radius Authentication

The Unified Identity Authentication Management system also integrates the standard Radius authentication service to authenticate some devices that support Radius authentication, such as VPN and firewall network devices and hosts. This will eliminate the need for these devices to maintain their own set of user identities.

3.9 Customize Authentication

In addition to the above built-in authentication methods, the platform also provides service and interfaces to develop custom authentication methods.

4. System function

The functional structure of the system is shown in the figure below:

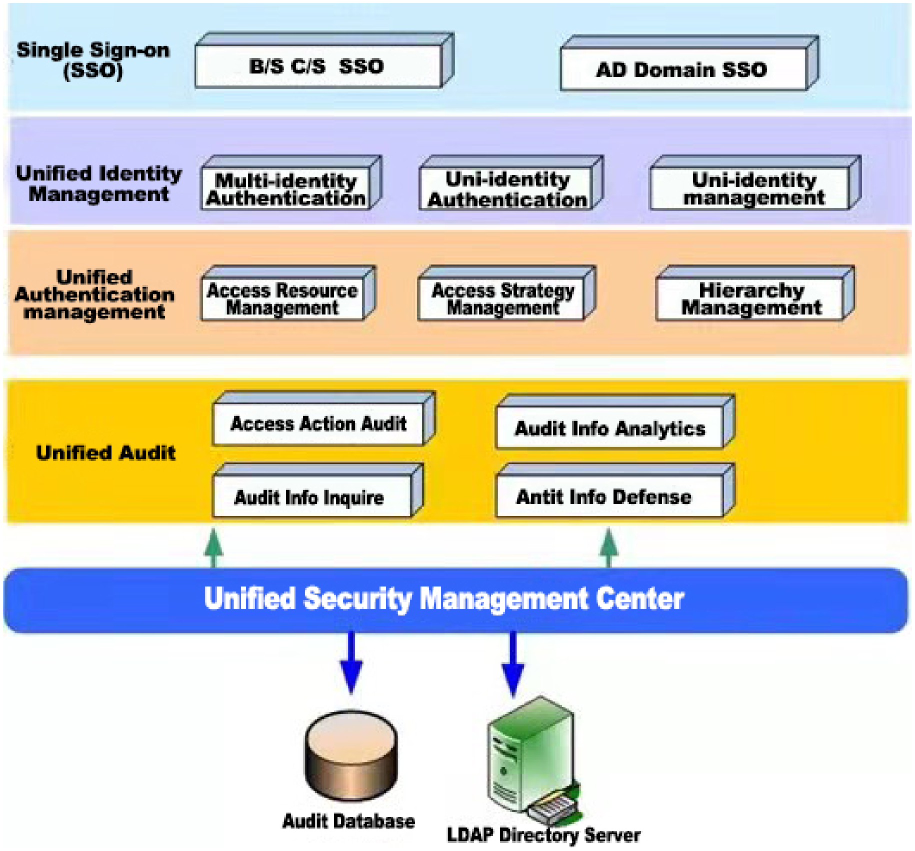

Figure 1. Structure of the system.

4.1 Single Sign-on (SSO)

Users only need to log in once to access all the systems that they have authorized. After their USB Key, digital certificate, or static password is authenticated by the unified authentication platform, users can access all application systems. The user does not need to enter the login password of the original system. The username and password of each application system in the background can be different. It simplifies the login process and saves the time of switching between systems. The user no longer needs to remember many passwords. The unified authentication platform convenient users access to the system.

B/S Structure Based Application System SSO: For B/S structured application systems, users only need to log in to the Web browser once to access the Web application systems with multiple user permissions through single sign-on (SSO) of the Unified Identity Authentication Management system. The user doesn't need to enter usernames and passwords one by one. The system does not need to change for the B/S structure of SSO implementation of transparent forwarding technology. The background system development platform, development structure has no relationship.

SSO & Domains Combined: The unified identity management system's SSO can be integrated with the domain and does not need to maintain its own user information. Users in the unified identity management system directly use the user identity information in the AD domain. The unified identity management system's SSO can divide users based on their departments and roles.

SSO implements a single sign-on between the Unified Identity Authentication Management system and the AD domain. After a user logs in to the AD domain, the user can access all accessible systems without re-entering the username and password.

4.2 Unified Authentication

Without changing the application system, the administrator can authenticate users on all systems (B/S) in the integrated system uniformly. The administrator can also manage user information and authentication method uniformly by using the enhanced identity authentication method.

4.2.1 Strong Identity Authentication

In the face of various insecure problems of traditional static passwords, the platform of the Unified Identity Authentication Management system adopts enhanced identity authentication q1based on PKI technology. It supports digital certificate authentication and can use a soft certificate or USB Key authentication.

When users want to access protected application systems, strong identity authentication is required. Strong identity authentication includes a soft certificate stored on the computer or inserting a USB Key. The Unified Identity Authentication Management system verifies the certificate information. If the user does not pass the strong identity authentication, the access will be denied to the protected system. If strong identity authentication is passed, secure channels are established for users to access application systems.

In addition to digital certificate authentication, static password authentication is reserved. The interfaces are reserved for other authentication modes, such as dynamic password authentication and SMS authentication, to meet security requirements in different development stages.

4.2.2 Unified Identity Authentication

Before a user accesses an application system, the user must go to the unified Identity authentication management system for authentication. After the authentication, the user can access the internal application system. The process dramatically reduces the various security risks caused by the independent mutual certification between different internal systems.

4.2.3 Application Authentication Interface

The Unified Identity Authentication Management system provides an authentication interface. The newly developed application system can integrate with the Unified Identity Authentication Management system by calling the authentication interface. After the user passes the authentication on the Unified Identity Authentication Management system, the application system can recognize the user with its interface. The newly developed system does not need to establish a user database but only has a set of user identity information (username and password, or digital certificate identification) in LDAP.

Unified identity Authentication management system provides two types of authentication programming interfaces for applications.

Java programming interface can be used for Java-based application systems (including WEB application systems based on JSP and Java-based applications);

For other systems developed in non-Java language, the Unified Identity Authentication Management system provides an authentication interface in the form of web services to meet the requirements of cross-platform and independency of the development language of the application system. As a primary XML/HTTP communication mode, it can also communicate across firewalls.

To ensure the security and reliability of the authentication process, HTTPS can be used to encrypt the authentication process.

4.3 User Identity Management

Manage user identity information in a unified manner. To prevent security risks caused by the failure to delete expired user identity information promptly. Suppose an employee is dismissed or changed position. In that case, the change only needs to be made in the management center to restrict the employee's access to the background system and eliminate the threat of illegal access to the background system.

4.3.1 User Group Management

Users can be managed in groups and departments based on the internal organizational structure of the zone. The management of an organization can be divided into multiple levels. Sub-departments are set under one department, and users are organized under the sub-departments.

4.3.2 Hierarchy of User Management

Accounts can be set according to the internal organizational structure of the zone, and any multi-level departments, sub-departments can be created without limit.

Users can be managed at different levels by multi sub-administrators with different authorization levels. The authorization of sub-administrators can be set by the main administrator. The sub-administrators can be authorized to manage only users at this level or users at this level and below levels. The sub-administrators can be authorized to view, create, modify, and delete users that they are in charge of.

The system can specify one or more super administrators who can manage all users—relieving the management burden of the headquarters administrator and clearing management responsibilities in the zone.

4.3.3 User Account Management

The user account is generally divided into two parts: the user's unique ID and the user's account in each application system.

Unique User ID Management: Assign the user with unique IDs and strong identity authentication in the zone. Centrally manage user account information, including creating, modifying, deleting, and suspending accounts. If the above operations are made on an account, the access behavior of the account will change accordingly.

User system account management: Within the management platform, the account information of users in each system is saved. The system account can be assigned to users directly by the system administrator on the management platform. The administrator can also allow users to add themselves to the system via self-registered terminals. The system administrator can modify, query, and delete users' accounts in a unified manner.

4.3.4 User Information Model Management

Unified identity authentication management system unifies users into a standard user model, including:

A unique account of the user

Basic attributes: name, department, contact information, etc.

Advanced properties: roles, accessible application systems, accounts in each application system

Extended attributes: user's extended attributes can be added

4.3.5 Role Management

The authorization mechanism of the Unified Identity Authentication Management system is based on roles. Therefore, in the management center, various roles can be created, defined, modified, deleted, and queried according to the characteristics of the integrated system itself and the division of functions and powers. Users are also assigned to their roles, and roles are mapped by user ids. In authorization management, the administrator can assign resources to each role and set permissions for different roles.

4.3.6 Organization Unit Management

Unified identity authentication management system provides organization unit management function. It is different from the user management module that is based on zone organization structure management mode. It can be defined from a variety of perspectives to show the user information, such as the user tree.

4.3.7 User Self-registration Management

In order to improve management efficiency and reduce management costs, the Unified Identity Authentication Management system provides a web-based self-registration service function. The self-registration system allows users to register their basic information and account information in various application systems.

4.4 Role-based authorization management

4.4.1 Accessing Resource Management

Register all application systems that need to be protected in the zone on the Unified Identity Authentication Management system, describe and manage them. This section lists the user information in each application system, queries the user information in each system, and displays the user information authorized to access each resource in an intuitive way. Uniformly authorize all users. A role-based authorization mechanism is adopted to divide roles according to the internal organizational structure of the zone and bind roles for users. Assign different application systems to different positions to determine whether they can or cannot access a system. After authorization, only the systems they have access to will be displayed on the single sign-on platform.

4.4.2 Access Policy Management

Customize different access policies for various roles. An access policy includes the resources that can be accessed and access control rules. The administrator can set flexible access rules, such as by time segment or network segment. Different policies can be customized according to suit a variety of situations, and access control can be implemented for different situations. Simple and advanced policy management modes are provided for different types of users, ensuring ease of use and flexibility.

4.4.3 Hierarchical Authorization Management

The unified identity management system can manage users at different levels. System administrators can manage and assign authorization to only users at the same level but users in other groups. The super administrator can manage all users.

A Unified Identity Authentication Management system at the same time can be accurate to the internal system of each module to the operation (watch, add, delete, change, check) permission management.

4.5 Account Synchronization

The Unified Identity Authentication Management system supports extracting user information directly from the relational database and importing account information through Excel. User information can be synchronized from LDAP. Support for importing user information from Domain; Users in the AD can be referenced as local users.

The unified Identity management system uses local user identity information as the user identity source and writes local users to other relational databases, LDAP, Domain, and AD.

4.6 Approval Management

The Unified Identity Authentication Management system can approve various operations, easily customize multiple approval processes for approval, rely on the approval process, joint approval, etc. The examination and approval methods include single person examination and approval, multi-person examination and approval, and majority examination and approval; The approval processing methods include rejection, approval, forwarding approval, timeout processing etc.

4.7 Unified Audit

The audit is an indispensable part of information system security precautions. Establishing a comprehensive and effective traceability mechanism requires reliable recording of end-user and administrators' access processes. The system administrator can monitor the access status of users to the application systems in the zone in real-time and find out the illegal access events in time. It is also of great significance for the traceability and accountability of problems. In addition, real-time monitoring and auditing of system running status can enhance system maintainability.

4.7.1 Auditing Access Behaviors

The security audit subsystem audits behavior from three sources:

Audit the management behaviors of unified identity management system administrators

Administrators log in to and log out of the system

All management actions of the administrator are recorded as follows

The person responsible for the operation

Date and time of operation

Operation kind

Operations, such as changing user information, managing permissions, and managing authorization policies

Audit the access behaviors of common users

The behavior of a user to connect to the Unified Identity Management System platform

Login and logout time

Failed access attempts, such as identity information or unauthorized access

User access to the application system

Applications the user access

Login and logout time for each application

Operations performed by a user on an application system

Audit the operation of the Unified Identity Authentication Management system

Connection number out

Network anomalies

Other system exceptions

Load statistics: The unified identity management system serves to protect the number of user access and concurrency statistics, monitoring the system load status.

4.7.2 Blacklist Function

For users who attempt illegal access or malicious attacks, once the number of illegal connection attempts from the same IP address exceeds a certain number, the IP address is blacklisted and recorded in the audit database. The system will not accept access from this IP address for security review.

4.7.3 Querying Audit Information

The audit system of the Unified Identity Authentication Management System provides the powerful log query function, which can be queried by abnormal events or a combination of common events. The query categories are as follows:

The user accounts

Protected systems

Date/time

Abnormal event type

4.7.4 Analyzing Audit Information

The audit information analysis and statistics can be divided by time, event, secure system, and user account. The results are displayed in reports or graphs to help the administrator quickly and intuitively grasp security events.

By analyzing the system running audit information, the administrator can quickly find out the cause of the exception and restore the system in a timely manner.

4.7.5 Tamper-Proof Audit Information

By signing the saved audit information prevent the audit content recorded by the system from being modified manually. If the audit content is modified, the audit information is displayed with a special label and displayed to the management personnel in an intuitive way.

5. System deployment

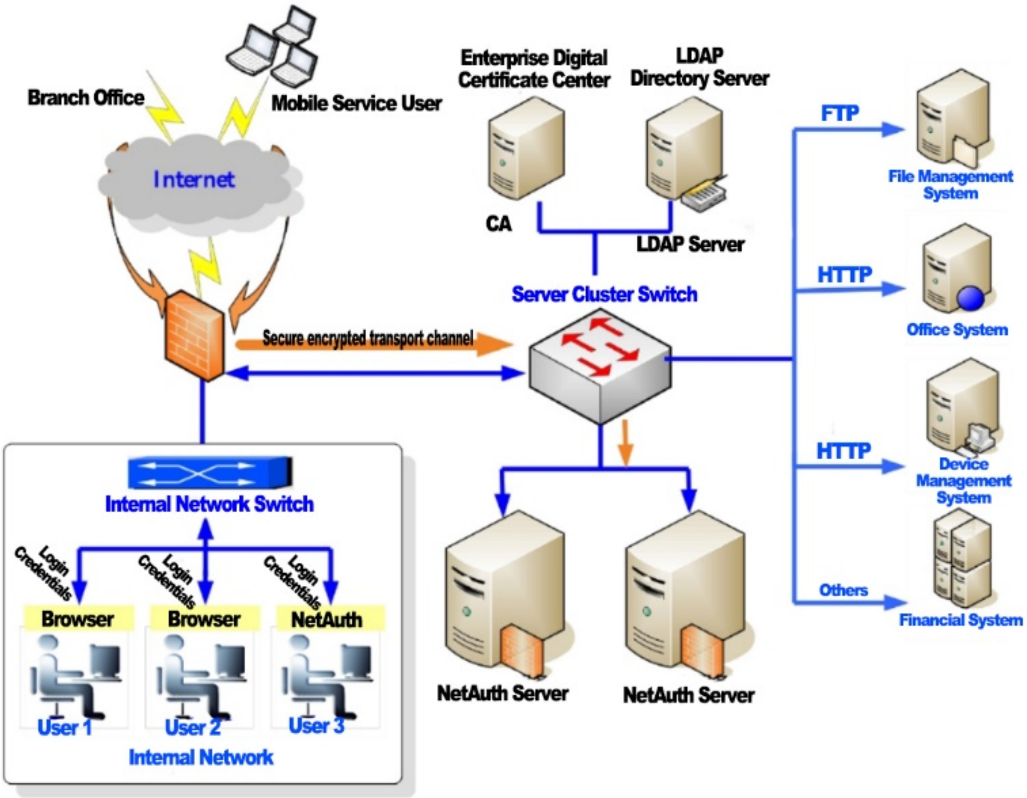

Figure 2. System network deployment diagram.

The deployment does not affect the network structure and combines with application systems through address mapping.

Its own firewall function, or deployed in the enterprise internal network firewall, ensures the security of its own and internal application system.

For a large number of users, hot standby can be deployed.

At the same time, the NetCert CA system can be deployed to issue digital certificates and implement enhanced identity authentication and encryption.

You can deploy an LDAP directory server as a tool for unified identity information storage and management for enterprise users. The LDAP user information directory server of the Unified Identity Management system can also be deployed on the same server as the unified Identity Management system.

6. The system characteristics and discussions

6.1 Application Independence

Protect all types of applications. The system protects applications based on various protocols, platforms, and development languages.

6.2 High Security

NetCert CA, a digital certificate authentication system, is used to issue digital certificates to users and is compatible with third-party CA certification bodies issued.

The built-in firewall security defense mechanism ensures system security and service system security.

Mobile users can use the encryption mechanism to encrypt the data transmitted over the network when accessing the internal system for secure remote access.

6.3 High Reliability

The Unified Identity Authentication Management system supports active/standby deployment if the number of users is significant to prevent failure. Users can deploy multiple Unified Identity Authentication Management system servers on the network to balance authentication requests among different servers.

6.4 Scalability

For users' needs, the system can be customized according to enterprises' characteristics and situations to achieve different functions.

Different development APIs are provided. Authentication APIs can be used to integrate the authentication of application systems into the Unified Identity Authentication Management system. In addition, other authentication methods, such as dynamic password authentication and reserved interfaces, are used to meet the authentication requirements of the zone.

For the newly constructed application system to provide open standard interface specifications, under the guidance of this standard, the application can be fully integrated into the unified management of the Unified Identity Authentication Management system platform to achieve unified authentication, single sign-on.

6.5 Cross-platform

Based on J2EE technology: the system is developed based on J2EE technology and has nothing to do with the platform. It can be conveniently implemented on any operating system and has good compatibility with other systems.

LDAP technology: provides powerful cross-platform and cross-application management capabilities and provides a basis for other systems in the zone to share resources. It is also convenient for other application systems to adopt the same standard development into a Unified Identity Authentication Management platform.

References

[1] J. Cao, Z. Li, Q. Luo, Q. Hao and T. Jiang, "Research on the Construction of Smart University Campus Based on Big Data and Cloud Computing," 2018 International Conference on Engineering Simulation and Intelligent Control (ESAIC), 2018, pp. 351-353, doi: 10.1109/ESAIC.2018.00088.

[2] H. Pinggui and C. Xiuqing, "Design and Implementation of Campus Security System Based on Internet of Things," 2017 International Conference on Robots & Intelligent System (ICRIS), 2017, pp. 86-89, doi: 10.1109/ICRIS.2017.28.

[3] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks and K. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 847-870, April 2018, doi: 10.1109/JIOT.2018.2802704.

[4] Q. Xu, X. Xiong, G. Feng, M. Guo and L. Wan, "Design of Intelligent Campus Multimedia Interactive System Based on Internet of Things Technology," 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), 2019, pp. 223-226, doi: 10.1109/ICVRIS.2019.00062.

[5] I. Hossain, D. Das and M. G. Rashed, "Internet of Things Based Model for Smart Campus: Challenges and Limitations," 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), 2019, pp. 1-4, doi: 10.1109/IC4ME247184.2019.9036629.

[6] L. Wei, "Campus Management Strategy Research under the Environment of Big Data," 2016 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), 2016, pp. 195-199, doi: 10.1109/ICITBS.2016.56.

[7] Y. Feng, W. Chen, Y. Zhang, G. Yu, Y. Liu and H. Xu, "Research on the Architecture of Smart Campus System Based on Data Middleground in University," 2021 IEEE 3rd International Conference on Computer Science and Educational Informatization (CSEI), 2021, pp. 18-21, doi: 10.1109/CSEI51395.2021.9477638.