Scholar Publishing Group
International Journal of Big Data Intelligent Technology
https://doi.org/10.38007/IJBDIT.2026.070104
ISSN 2790-0932 Vol. 7, Issue 1: 28-34

Security Improvement and Application of Identity and Access Management in Saas Platform

Qingyang Zhang

Simon Business School, University of Rochester, Rochester 14627, NY, United States

Keywords: SaaS platform; Identity and Access Management (IAM); multi-factor authentication

Abstract: With the widespread application of SaaS platforms in various enterprises, Identity and Access Management (IAM), as the core mechanism for ensuring platform security and user data privacy, is facing multiple challenges such as multi tenant environments, complex permission configurations, and integration of third-party interfaces. This article analyzes the functional scope and architecture composition of IAM on the architecture of SaaS systems, deeply discusses the main security issues that IAM faces in practical use, and proposes targeted solutions such as multi factor authentication, zero trust architecture, and unified identity system. The aim is to build an efficient, secure, and scalable IAM system suitable for SaaS platforms, enhance the overall platform's security and customer trust, and provide theoretical support and practical reference.

1. Introduction

With the rapid development of cloud technology, the Software as a Service (SaaS) model has become the digital foundational support for enterprises, and can be widely applied in fields such as finance, education, and healthcare due to its scalability and agile deployment advantages. However, the existence of many features such as multi tenant architecture, remote access, and third-party system integration has brought unprecedented security challenges to identity and permission management. Identity and Access Management (IAM) is the most fundamental mechanism for ensuring the trustworthiness of user identities and compliance with resource access, making it the most important security aspect of SaaS service platforms. Traditional IAM technology has a series of drawbacks when facing complex access relationships, such as insufficient authentication strength, chaotic access permissions, and difficulty in real-time auditing. Therefore, there is an urgent need for new technologies and strategies to address this issue. This article will systematically analyze and explore the construction status, main security issues, and security solutions of the SaaS service platform IAM, in order to improve platform security, provide theoretical basis and empirical suggestions.

2. Overview of SaaS Platform and Identity Access Management Theory

SaaS (Software as a Service) is the most important way of providing cloud computing services, and its advantages such as high reliability, low maintenance costs, and flexible scalability are widely used in many aspects such as commercial office, customer contact, and financial management. However, due to the multi tenant architecture and open access mode of SaaS platforms, it poses a huge challenge to their identity security protection. Therefore, the purpose of establishing an Identity and Access Management (IAM) system is to provide important guarantees for user authentication and resource authorization, and its design and deployment have a decisive impact on the security of the entire platform. Generally speaking, IAM systems include multiple functional systems such as identity identification, authentication technology, permission management, and access auditing. However, due to the increasing demand for access, traditional rigid permission allocation is no longer suitable for dynamic and changing business scenarios. The new IAM system focuses on unified identity identification, multi factor authentication, precise authorization, and policy based access control, adapting to the dynamic and security governance requirements of "who can access what" in SaaS environments. Building an efficient, secure, and easily scalable IAM framework has become the main approach to enhancing security architecture performance in SaaS service platforms.

3. Construction of IAM system framework in SaaS platform

3.1 Identity Management System Architecture

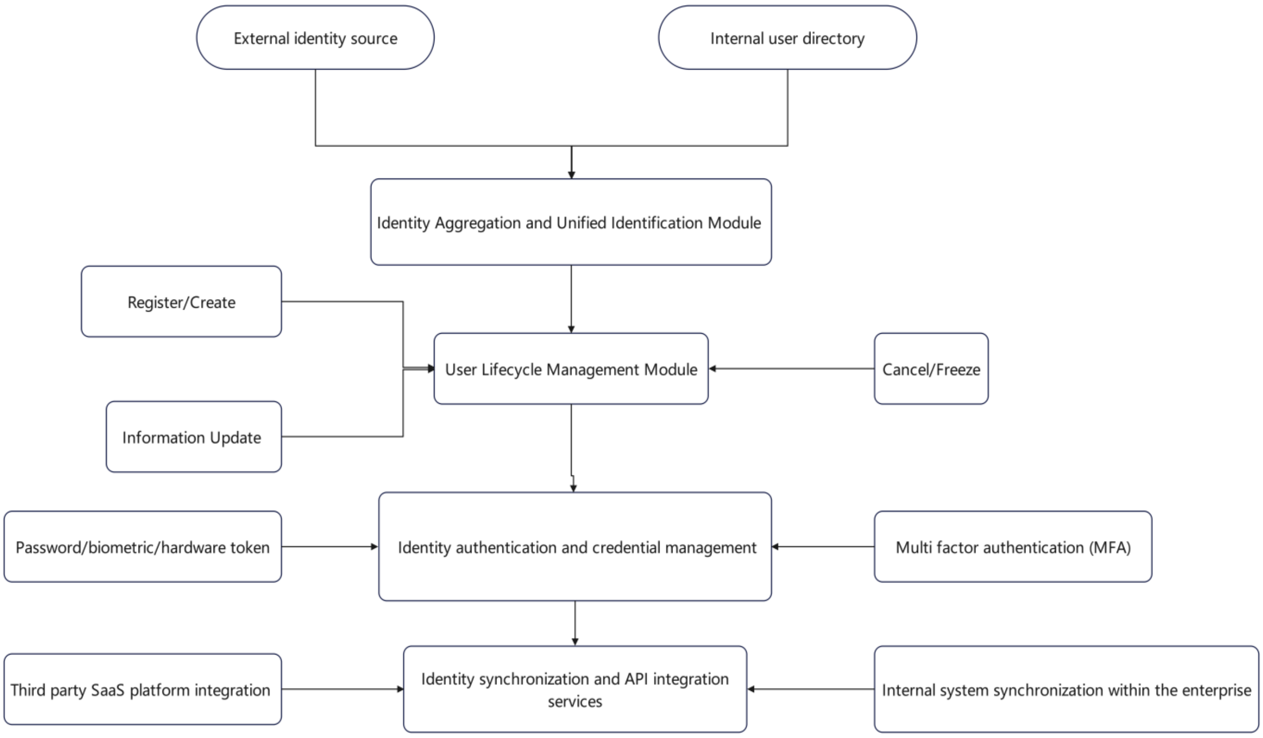
External identity source
Internal user directory
Identity Aggregation and Unified Identification Module
Register/Create
User Lifecycle Management Module
Cancel/Freeze
Information Update
Password/biometric/hardware token
Identity authentication and credential management
Multi factor authentication (MFA)
Third party SaaS platform integration
Identity synchronization and API integration services
Internal system synchronization within the enterprise

Figure 1 Identity Management System Architecture Framework Diagram

The identity management system is the core of the IAM system, responsible for the unified management of all processes related to user identity creation, management, verification, and cancellation. In the SaaS environment, the identity management system needs to be designed for multi tenant architecture, with different systems and roles requiring authentication. Its main components include: identity directory service, lifecycle management, unified identity identification, identity synchronization strategy, etc. Firstly, identity directory services typically store users' basic data, role information, and authentication credentials in identity databases such as LDAP, Active Directory, or cloud environments. Secondly, user lifecycle management covers user registration, change, cancellation, and other operations, requiring dynamic adjustment and real-time synchronization of permissions at each stage. Thirdly, the purpose of unified identity technology is to ensure that users can maintain the same identity correspondence during cross platform and cross service access, avoiding the occurrence of "identity fragmentation". Fourthly, in order to meet the diverse authentication requirements of different types of authentication methods such as enterprise SSO, modern identity management systems can also interact with external identity service providers (such as OAuth, OpenIDConnect, SAML).

3.2 Access Control Model and Authorization Mechanism

The access control model and authorization mechanism are key components of the IAM system, with the core responsibility of ensuring that only authenticated users have access and limiting illegal use of sensitive data and critical operations. In SaaS platforms, access control needs to balance the isolation, dynamism, and auditability of multi tenant environments, often using various control models such as role-based access control (RBAC), attribute based access control (ABAC), and policy based access control (PBAC).

The RBAC model binds permissions to specific roles, allowing users to obtain corresponding permissions by assigning roles, thereby reducing permission management. The ABAC model is completed through real-time evaluation of user attributes, resource attributes, and environment attributes, so it can achieve flexible permission control. In recent years, with the increasing complexity of cloud environments, the PBAC model based on security policies has emerged, characterized by real-time authorization and management using contextual information with security policies as the core. In practice, SaaS servers can mix multiple models and combine various technical means such as multi factor authentication (MFA), minimum privilege principle, session control, and access validity period to enhance the system's security capabilities and dynamic adaptability of permission configuration. And it is necessary to design a comprehensive authorization change audit and abnormal access alarm mechanism to enhance the controllability and transparency of overall access management.

3.3 Integrated Mechanism for Security Audit and Event Response

Security auditing and event response are key reinforcement modules of the IAM system, which mainly implement tracking and analysis of user operations, as well as automatic emergency response measures when abnormal situations are discovered. In SaaS platforms, due to their openness and multi tenancy characteristics, the security audit system should be comprehensive and flexible, covering various key tasks such as identity authentication, permission management, information retrieval, etc. It should also have complete multi system log collection capabilities and timely risk detection capabilities. The audit system consists of three modules: operation log collection, behavior analysis, and compliance report generation. They can effectively help the system identify high-risk events such as invalid login, unauthorized use, or illegal acquisition of sensitive information, and cooperate with event response mechanisms to perform established automatic isolation, event notification, and mandatory logout actions, better achieving proactive and real-time security protection. At the integration level, modern SaaS platforms often integrate IAM systems with security information, event management (SIEM), intrusion detection systems (IDS), and other tools to achieve unified log centralized management and security situational awareness.

3.4 System Integration and Platform Adaptation Mechanism

In the cloud based Software as a Service (SaaS) model, Identity and Access Management (IAM) systems not only need to have internal identity and permission management capabilities, but also need to achieve seamless integration with various business systems and third-party platforms, in order to build a unified identity management and access control system. The core of system integration is to establish a complete set of identity authentication, authorization, and access processes using standard protocols and matching methods. Common integration methods include using protocols such as OAuth2.0, SAML, OpenIDConnect to implement single sign on (SSO) and cross domain authentication to ensure that users can maintain continuity and security of their identity during the transition to other systems. At the same time, the IAM platform is equipped with standard API interfaces that support the access of other modules such as API gateways, security policy engines, logs, and audits to form a unified security monitoring system. In addition, due to the differences between different SaaS platforms, adapter mechanisms need to be used to enable personalized authentication processes and corresponding permission models in multi tenant environments. By building a highly modular and open IAM system architecture, the platform can flexibly support business expansion and diversified service access while ensuring security.

4. The main security issues faced by IAM in SaaS platforms

4.1 Identity isolation challenges in multi tenant environments

In SaaS platforms, multi tenant architecture enables multiple organizational users to share the same physical resource pool, which can improve resource utilization but can also pose security risks to the entire system, such as identity isolation and ambiguous permissions. Due to the fact that data, identity directories, and access policies among tenants are often deployed on the same platform, without effective identity isolation for users, there are risks such as identity mixing among different organizational structures, cross tenant access by users from different organizations, and incorrect authorization. Typical problems include conflicts in user unique identifiers between tenants, confusion in permission inheritance relationships, and lack of directory isolation logic. When the centralized authentication portal cannot meet the diverse needs of different tenants, problems may arise. For the sake of deployment efficiency, some systems adopt a common database architecture, which makes logical isolation more difficult.

Table 1 Common problems and manifestations of identity isolation in multi tenant environments

Question type	Expressions	Security risks
Identity conflict	Different tenant users use the same username/ID	Causing authorization errors or information leakage
Chaotic inheritance of permissions	The same role has different permissions in different tenants	Misuse of permissions, difficult to hold accountable
The directory logic is not isolated	User information is stored in a shared directory structure	Easy occurrence of unauthorized access or data mixing
Unified authentication policy failure	Unable to dynamically load access control and login policies based on tenants	Unable to customize tenant strategy, increase attack surface

4.2 Complex Access Permission Configuration and Abuse Risk

In SaaS platforms, the configuration of access permissions typically requires consideration of multiple factors such as user roles, organizational structure, and application scenarios. Due to the high flexibility of permission control design, the large demand for tenant customization, and the frequent dynamic changes in role and resource mapping, it is difficult to configure and maintain permissions, the cost of control is high, and it leads to the occurrence of "exceeding authority", "abuse of authority", and illegal access to data. Some platforms do not adopt refined authorization mechanisms and only provide coarse-grained role control functions, which do not meet the increasingly changing access requirements and compliance requirements. At the same time, if the administrator neglects permission management, it can also bring huge harm. Once a high permission account is abused, it will cause serious consequences.

Table 2 Typical Problems of Complex and Abusive Access Permissions Configuration on SaaS Platforms

Question type	Expressions	Potential risk
Redundancy of permissions	Users retain their original permissions even after leaving their posts	Causing unauthorized access and unauthorized operations
Chaotic authorization path	The role inheritance chain is unclear, and the source of permissions is unknown	Inability to hold accountable and audit
Abuse of high authority	Administrator's unauthorized operation without approval mechanism	Data leakage, system configuration tampering
Lack of minimum permission control	The default permission settings are broad and lack a dynamic adjustment mechanism	Improve attack surface and affect business security isolation

4.3 Identity security risks brought by third-party integration interfaces

To meet the needs of customers for multi system collaborative work, SaaS platforms generally integrate the system with third parties through APIs, OAuth protocols, or using public identity identifiers (such as OpenIDConnect). This convenient method may bring a series of security risks, such as introducing an elongated authentication chain, increasing the risk of credential exposure, weak interface permission control, and other security risks. Especially under the three-layer trust relationship of "platform third-party end user", if security control measures such as identity authentication, signature verification, and access frequency control for interface operations are not considered, attackers can impersonate or expand their permissions through interface modification, token replay, session fixation, and other methods. In addition, some SaaS platforms do not implement the principle of minimizing permissions for third-party services, which gives third parties excessive access permissions and increases the risk of identity leakage.

Table 3 Common Identity Security Issues in Third Party Interface Integration

Question type	Expressions	Security risks
Voucher exposure	Static API Key or Access Token exposed in the client or URL	Can be intercepted and used to forge access
Signature mechanism missing	Request not signed or weak verification logic	Attackers can replay or tamper with request content
Extensive access control	Third parties have extensive read and write permissions without fine-grained restrictions	Easy to trigger unauthorized or illegal data access
Lack of interface audit	Lack of call logs and behavior monitoring	Difficult to trace security incidents and delayed response

5. SaaS Platform IAM Security Enhancement and Application Strategy

5.1 Deploying Multi Factor Authentication and Dynamic Permission Management Mechanism

To address the issues of identity isolation and privilege abuse in multi tenant environments, SaaS platforms need to deploy Multi Factor Authentication (MFA) and dynamic access control mechanisms. Multi factor authentication combines passwords, biometric identification, and one-time tokens to enhance account security. Dynamic access control is the real-time dynamic permission adjustment based on the subject's behavior and background (time, location, client, etc.), achieving "on-demand authorization" and "real-time retrieval".

For example, in a certain enterprise document collaboration SaaS platform, in order to prevent high privilege accounts from being targeted by phishing attacks, the platform introduces the following dynamic permission assessment function based on contextual risk scoring:

$$R = \alpha \cdot L + \beta \cdot D + \gamma \cdot T \tag{1}$$

Among them, R: Access risk score; L: Reliability rating of login location; D: Device fingerprint reliability; T: Sensitivity of access time period; α . β , γ : are weighting coefficients adjusted according to business scenarios. When the risk score R exceeds the set threshold, the system will forcibly enable MFA or restrict the user's access range.

5.2 Building a Zero Trust Architecture and Strengthening Access Control Mechanisms

The traditional "boundary protection" security concept is no longer able to meet the dynamic, distributed, and multi tenant access requirements in SaaS platforms. Zero Trust Architecture (ZTA) is based on the principle of "never trust, always verify", emphasizing authentication, device confirmation, and behavior evaluation for every access request, thereby achieving fine-grained and persistent access control. Building a zero trust architecture in SaaS platforms requires encapsulating access decision elements based on user, device, content (access type), geographic location, and other information, and implementing real-time access authorization through policy based access management. For example, when the system detects abnormal access patterns of "device changes+high traffic" through behavior model analysis, it triggers permission contraction or mandatory authentication process. Subsequently, the zero trust architecture emphasizes network segmentation and minimal resource exposure. The platform can establish a service grid between microservices to perform API level request confirmation and access isolation work. At the same time, security components such as authentication gateways, precision access proxies, and behavior aware engines are introduced to establish and form a continuous automatic response mechanism based on trust evaluation, thereby enabling access control mechanisms to be unaffected by single point authentication technology and forming a complete secure lifecycle.

5.3 Establish a unified identity platform and gateway collaborative protection mechanism

In SaaS platforms with multiple system integrations, authentication and interface security are often disconnected, which can easily lead to access links being exploited by attackers. For the purpose of consistency based on identity authentication and interface protection, it is necessary to build a unified identity authentication platform and use API gateways to achieve an integrated security protection mechanism that includes user identity authentication, permission authorization, and interface invocation. The unified identity platform can integrate local databases, social media accounts, and enterprise single sign on services, and provide a universal identity authentication portal and identity token management platform for all application services. In addition, standard protocols such as OAuth2.0 and JWT are used to issue short-term access tokens to each subsystem, ensuring that access activities are traceable and revocable.

For example, a large educational application software cloud service platform integrates a large number of third-party information provision services. The platform uses Keycloak as an identity recognition system and uses API gateway Kong to complete the verification links of various services. The operation steps are as follows: when the user logs in using the unified entrance, they will receive a token; The API gateway will verify the token before each called interface, and determine whether it can be used based on the role data information contained in the token, effectively preventing unauthorized calls and forged requests.

6. Conclusion

Against the backdrop of rapid adoption of SaaS platforms and increasingly complex multi tenant architectures, Identity and Access Management (IAM) has become an important component in building a network security system. This article summarizes the system architecture, security threats, and solutions of IAM, and proposes key mechanisms such as multi factor authentication, zero trust architecture, and unified identity platform. Through analysis of technology, it is found that only by organically integrating identity authentication, permission control, and interface protection into a cyclic management process can the flexibility of the system be ensured and security risks be effectively contained. In the future, IAM systems will further leverage intelligent technologies such as artificial intelligence, behavior analysis, and automatic response capabilities to evolve towards intelligence and dynamism, ensuring the connectivity of SaaS services and data security.

Reference

[1] Vegas J, Llamas C. Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments. Future Internet, 2024, 16(12):469-469.

[2] Glöckler J, Sedlmeir J, Frank M, et al. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering, 2023, 66(4):421-440.

[3] Wu Y, Pang M, Ma J, et al. An Identity Management Scheme Based on Multi-Factor Authentication and Dynamic Trust Evaluation for Telemedicine. Sensors, 2025, 25(7):2118-2118.

[4] Cambou F B, Alam M. Challenge–Response Pair Mechanisms and Multi-Factor Authentication Schemes to Protect Private Keys. Applied Sciences, 2025, 15(6):3089-3089.

[5] Sousa J D M, Gondim L R P. A multi-factor user authentication protocol for the internet of drones environment. Peer-to-Peer Networking and Applications, 2025, 18(2):69-69.

[6] Lu, Z. (2025). AI-Driven Cross-Cloud Operations Language Standardisation and Knowledge Sharing System. European Journal of AI, Computing & Informatics, 1(4), 43-50.

[7] Yu, X. (2025). Application Analysis of User Behavior Segmentation in Enhancing Customer Lifetime Value. Journal of Humanities, Arts and Social Science, 9(10).

[8] Zheng, H. (2025). Research on Delay-aware Scheduling Algorithms for Edge Task Migration in High-concurrency Environments. Engineering Advances, 5(4).

[9] Li, J. (2025). The Impact of Distributed Data Query Optimization on Large-Scale Data Processing.

[10] Dingyuan Liu. The Relationship between Household Consumption Pattern Changes under Disasters and the Recovery of Business Ecosystems. Academic Journal of Business & Management (2025), Vol. 7, Issue 12: 151-156.

[11] Lu, Z. (2025). Design and Practice of AI Intelligent Mentor System for DevOps Education. European Journal of Education Science, 1(3), 25-31.

[12] Zheng, H. (2025). Research on Lifecycle Configuration and Reclamation Strategies for Edge Nodes Based on Microservice Architectures. Advances in Computer and Communication, 6(5).