Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 8, No.1, August : 2025

A FRAMEWORK-AGNOSTIC AND SCALABLE IDENTITY MANAGEMENT PLATFORM FOR SECURE USER AUTHENTICATION AND ACCESS CONTROL

Mrs.T.Rani Mangammal, Assistant Professor, Dept.Of Computer Science, SSM Institute of Engineering and Technology, Dindigul, India. ssmcserani@gmail.com
Jeyaraman S, Computer Science and Engineering, SSM Institute of Engineering and Technology Dindigul,India. jeyaraman.saravanan23@gmail.com
Jeya Shree S, Computer Science and Engineering, SSM Institute of Engineering and Technology Dindigul,India. jeyashreeselvan9@gmail.com
Kajalakshmi M, Computer Science and Engineering, SSM Institute of Engineering and Technology Dindigul,India. mkajalakshmi@gmail.com
Karpagam S, Computer Science and Engineering, SSM Institute of Engineering and Technology Dindigul,India. selvarajkarpagam234@gmail.com

ABSTRACT
The web and mobile applications increase in complexity and demand increased security, secure and scalable Identity and Access Management (IAM) systems are a necessity. Conventional IAM solutions rely on inflexible, framework-specific SDKs and downloads, which significantly reduce flexibility, ease of integration, and overall platform independence. This paper presents a new, framework-independent IAM platform using a redirect-based authentication model that effectively removes such dependencies. Built with a solid and modern technology stack-consisting of Spring Boot, MongoDB, JWT, OAuth 2.0, Multi-Factor Authentication (MFA), and React-the platform is designed for easy, efficient integration with both web and mobile applications. It offers multilayered security, completely customizable team- and role-based access control, adaptive authentication interfaces, user-friendly configuration, and AI-driven real-time security monitoring. The system architecture, development approach, key design decisions, and a comparative analysis with current IAM offerings are discussed. Experimental outcomes show appreciable enhancements in integration ease, cross-platform portability, system performance, branding alignment, and overall security strength and reliability.

Keywords: Identity Management, Access Control, Authentication, Security, Scalability, JWT, OAuth 2.0, MFA, Framework-Agnostic IAM, Role-Based Access, Branding, AI Monitoring, Mobile Integration.

I. Introduction
In the modern digital landscape, web applications are increasingly targeted by sophisticated cyber threats, making robust security a paramount concern for organizations. As businesses and institutions migrate their operations to the digital realm, the need to safeguard sensitive information and ensure authorized access has never been more critical. Identity and Access Management (IAM) systems play a pivotal role in this context, providing the necessary mechanisms to authenticate users and control access to resources. Traditional IAM platforms, however, often come with significant limitations. They frequently require developers to integrate specific frameworks and SDKs, which can be complex and time-consuming, thereby reducing flexibility and increasing integration costs. This complexity can act as a significant barrier for organizations, particularly smaller ones, looking to implement secure and scalable IAM solutions. The challenges associated with integrating IAM systems are compounded by the rapid evolution of web technologies and the growing demand for solutions that can adapt to diverse and dynamic environments.
The proposed solution aims to address these challenges by introducing a novel IAM platform that is both frame work agnostic and scalable. This platform leverages a robust tech stack, including Spring Boot, MongoDB, JWT, OAuth 2.0, MFA, and React, to provide a flexible, secure, and scalable IAM solution. The platform's framework-agnostic approach simplifies the integration process by providing

a unique link that can be embedded in any landing page, eliminating the need for complex coding and framework-specific integrations. This innovative approach not only enhances security but also ensures that the platform can be easily adopted and implemented by organizations of all sizes. The platform's multi-layered security features, including Time-Based One-Time Passwords (TOTP) for Multi-Factor Authentication (MFA), further bolster its security capabilities. Additionally, the platform offers seamless multi-role and team management, customizable login and sign-up interfaces, and personalized authentication UIs to match customer branding, thereby enhancing user experience and brand continuity.

II. Literature

Identity and Access Management (IAM) plays a central role in safeguarding modern digital systems. As organizations increasingly rely on digital infrastructure to store and manage sensitive data, IAM systems become essential in ensuring that only authorized users can access specific resources. These systems manage user identities, define access levels, and enforce security policies to prevent data breaches and insider threats.

IAM solutions are not just a technical necessity; they are a critical aspect of organizational governance and risk management. They help ensure data integrity, protect intellectual property, and maintain compliance with industry standards and government regulations such as GDPR, HIPAA, and ISO standards. With the rapid growth of cloud computing, remote work, and online services, IAM has become the backbone of secure digital interactions.

In web applications, IAM is responsible for authenticating users, authorizing access based on roles or permissions, and logging user activity to ensure accountability. Organizations in sectors like finance, healthcare, government, and education have long adopted IAM systems to manage their workforce and customer identities securely.

However, as cyber threats become more sophisticated and distributed systems grow in complexity, traditional IAM approaches must evolve. Modern IAM must support dynamic access control, real-time monitoring, and seamless user experiences, all while being scalable and adaptable to a variety of platforms and devices.

2.1 Existing IAM Solutions and Their Limitations

There are several commercial and open-source IAM solutions in the market today, including popular options like Auth0, Okta, Clerk, and Firebase Authentication. These platforms offer high security and convenient features, such as social login, multi-factor authentication, and role-based access control.

While powerful, these solutions often require developers to tightly integrate platform-specific SDKs and APIs. This leads to a strong dependency on particular frameworks or libraries, which can limit the adaptability of the application. The integration process may also involve significant development effort, increasing both time and cost for implementation.

For smaller organizations or startups with limited technical and financial resources, such high integration complexity can be a major barrier. Moreover, these platforms may impose usage- based pricing models that are not ideal for scaling applications affordably.

Another area of innovation in IAM is decentralized identity, often implemented using blockchain technologies. These decentralized IAM systems offer the potential to give users greater control over their digital identities and reduce reliance on central identity providers. However, such systems also

come with limitations, including a steep learning curve, performance constraints, and limited support for real-time, high-throughput applications.

These issues highlight the need for more flexible, cost-effective, and easy-to-integrate IAM solutions that are suitable for both small businesses and large enterprises. The ideal solution should reduce technical friction while providing robust security and scalability.These issues highlight the need for more flexible, cost-effective, and easy-to-integrate IAM solutions that are suitable for both small businesses and large enterprises. The ideal solution should reduce technical friction while providing robust security and scalability. In addition, most traditional IAM platforms lack seamless interoperability across diverse technology stacks, which can be problematic in heterogeneous environments. Organizations often face difficulties customizing authentication flows to suit specific business logic, as many platforms offer limited extensibility out of the box. vendor lock-in is another concern, as migrating from one IAM provider to another often involves significant re-engineering of the authentication architecture. This lack of portability restricts long-term strategic choices for developers and business leaders alike. Furthermore, compliance with regional data protection laws such as GDPR or HIPAA can be challenging when using third-party IAM providers, particularly those hosted in different jurisdictions. This introduces legal and operational risks.

2.2 Advancements in IAM Technologies

Recent innovations in IAM technologies have significantly strengthened the ability of organizations to secure digital identities and data. Multi-Factor Authentication (MFA) has become a standard approach for reducing the risks associated with password-based authentication. MFA requires users to verify their identity using two or more factors— something they know (password), something they have (smartphone or token), or something they are (biometrics).

One of the most widely adopted forms of MFA is the Time-Based One-Time Password (TOTP), which generates a new, time-limited code every few seconds. Even if a password is compromised, attackers cannot gain access without the valid TOTP.

Beyond MFA, Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being applied to IAM for threat detection and anomaly analysis. These systems monitor user behavior, identify suspicious activity, and respond in real time to potential threats. For instance, if a user logs in from an unfamiliar location or device, the system might trigger additional verification steps or temporarily block access.

These advancements enhance IAM systems by providing a proactive, intelligent layer of defense against evolving cyber threats. They not only improve security but also enable adaptive, user-friendly experiences without compromising protection.

2.3 Gap Identification

Despite progress in the field, a notable gap exists in the development of framework-agnostic IAM solutions—systems that are not tied to a specific frontend or backend technology. Most existing IAM platforms require deep integration with particular SDKs or frameworks, which limits their flexibility across diverse technology stacks.

This tight coupling makes it challenging for developers who work with different stacks or want to adopt a microservices or decoupled architecture. Moreover, maintaining these integrations over time as the tech stack evolves can become a significant burden.

There is a clear need for an IAM solution that is lightweight, flexible, and framework- agnostic, capable of plugging into any application through standard protocols like OAuth2,

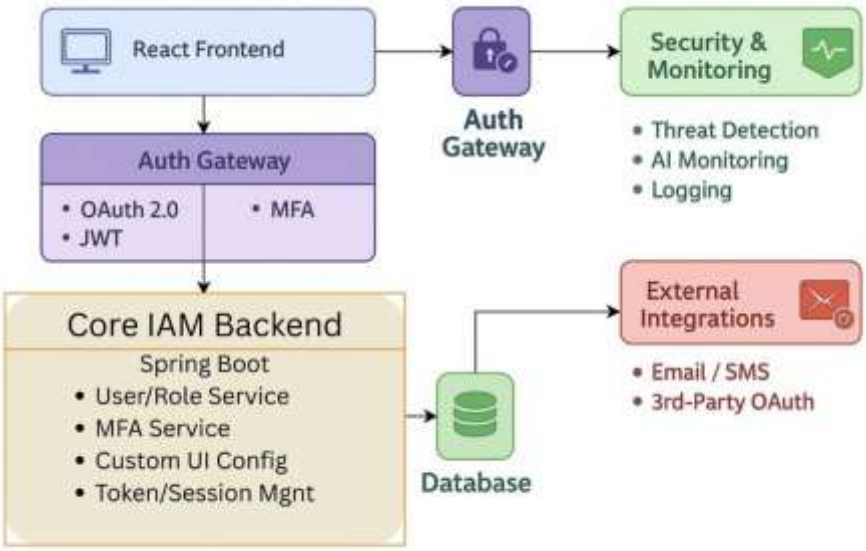
OpenID Connect, and simple API calls. Such a solution would offer a more universal, developer-friendly experience and reduce the time, effort, and cost involved in securing applications.

By focusing on framework independence, simplified integration, and modern security protocols, this research aims to contribute a versatile IAM platform that addresses the evolving needs of modern software systems and bridges the existing gap in identity management solutions.

Existing IAM solutions often have technical constraints, offering limited customization in user interfaces and user flows, making them less adaptable for businesses with unique branding or process requirements. Many lack modular architectures, reducing reusability across projects and slowing development cycles. Additionally, there is insufficient support for granular access control models like attribute-based access control (ABAC), which are essential for dynamic, context-aware authorization decisions. The absence of developer-centric documentation and tooling impedes rapid prototyping and testing, while limited integration with CI/CD pipelines complicates the automation of identity workflows in agile environments. Furthermore, the lack of built-in observability features—such as real-time logs, audit trails, and analytics—hinders monitoring and compliance in production systems. This research aims to address these gaps by proposing an IAM framework that embraces open standards, minimal dependencies, ease of use, and compatibility with modern development and deployment practices.

Existing IAM systems often face challenges such as limited customization, lack of modularity, and insufficient support for advanced access control models. These issues, combined with inadequate documentation and integration with modern development practices, hinder development and operational efficiency. This research proposes an IAM framework that overcomes these challenges, focusing on flexibility, ease of use, and broad compatibility.

2.4 Proposed System



The proposed Identity and Access Management (IAM) platform is architected to offer a flexible, secure, and scalable alternative to traditional and decentralized IAM systems. It is designed to minimize integration complexity while providing powerful features like multi- factor authentication, fine-grained role management, customizable user interfaces, and seamless API interoperability. This

modern IAM system addresses the limitations of existing solutions by offering a developer-friendly, modular, and highly adaptable platform that can fit into a wide range of applications and organizational environments.
At the core of the proposed platform is the authentication module, which manages user identity verification through a secure, standards-compliant mechanism. The platform employs industry-standard OAuth 2.0 for authorization and JSON Web Tokens (JWT) for session management.
The authentication process follows a redirect-based workflow. When a user attempts to log in or sign up, they are redirected to a secure login page hosted by the IAM system. This approach centralizes the authentication logic, ensuring that login credentials are processed in a controlled and secure environment. Once authenticated, the system issues a JWT, which the client application uses for subsequent requests. This token contains encrypted user data and role information, making it easy to authorize access without additional database queries. This mechanism is both secure and scalable, suitable for applications with high traffic and multiple user roles.

To bolster security, the platform incorporates Time-based One-Time Password (TOTP) based MFA. After entering their credentials, users are prompted to input a six-digit code generated by an authenticator app (such as Google Authenticator). This code is time-sensitive and changes every 30 seconds, drastically reducing the chances of unauthorized access through stolen credentials.
Additionally, CAPTCHA integration is implemented to protect against automated login attempts and brute-force attacks. CAPTCHA challenges ensure that only human users are able to interact with the login and sign-up processes, providing an added layer of security without significantly impacting user experience.

The proposed IAM system uses JWTs not just for authentication but also for enforcing Role- Based Access Control. Within the JWT, user roles (such as admin, manager, or general user) are embedded as claims. When the frontend or backend systems receive the token, they can immediately evaluate a user's permissions based on the encoded role.

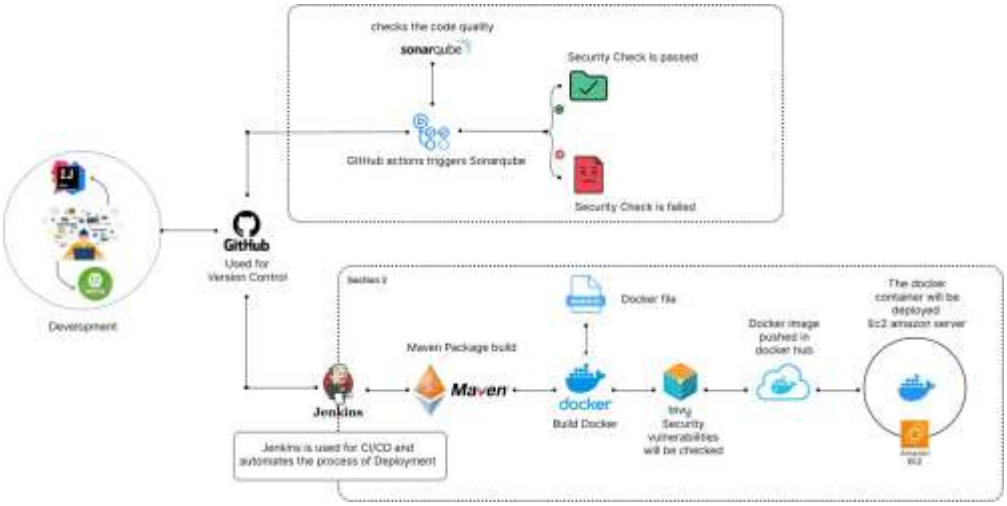
This built-in role management allows developers to implement fine-grained access rules directly within the client or server logic, without needing to repeatedly query an access control database. As a result, the system can efficiently manage secure access to sensitive resources and restrict functionality based on user roles, enhancing overall security and performance.

The platform offers powerful team and role management capabilities. Organizations can create hierarchical team structures, where each team or sub-team can have assigned roles and scoped permissions. This structure is especially useful for businesses that operate across multiple departments or projects, enabling fine-tuned access control within teams and collaborative environments.
For instance, an engineering team might have developers, testers, and team leads, each with a different set of permissions. These roles can be dynamically adjusted through the platform's interface or APIs, allowing organizations to easily adapt to changes in team structure or responsibilities without rebuilding their IAM framework.

User interface customization is another major feature of the proposed IAM platform. Organizations can personalize their login and sign-up pages to reflect their branding—adding logos, choosing color themes, and modifying form content.
This flexibility ensures a consistent brand identity across user-facing authentication screens, improving the user experience and fostering trust. Moreover, it allows organizations to deliver a cohesive visual interface regardless of whether the app is hosted on mobile, web, or other digital platforms.

To ensure seamless integration with third-party systems, the platform includes a fully- documented Open API. This API enables organizations to interact programmatically with the IAM platform for tasks such as user registration, token validation, role assignment, and account management.
Unlike traditional IAM providers that rely heavily on specific SDKs or frameworks, this platform's open API supports language-agnostic integration. Developers can use any backend

or frontend technology of their choice—Node.js, Python, Java, React, etc.—and still communicate smoothly with the IAM backend. This approach minimizes vendor lock-in, encourages system interoperability, and supports rapid development.
To further strengthen token security, each organization using the IAM platform is issued a unique public key. This key is used to verify the authenticity of JWT tokens issued by the platform. When a client or backend receives a JWT, it can validate the signature using this public key, ensuring the token is not tampered with or forged.
By allowing organizations to perform local verification of JWT tokens, the platform reduces dependency on real-time calls to the IAM service, improving performance and enabling offline token validation in distributed systems. This capability ensures a high level of trust and autonomy, especially in sensitive or high-security environments.



2.5 Advantages of Proposed System

The proposed Identity and Access Management (IAM) platform provides numerous advantages that significantly improve security, streamline access control, and ensure the solution remains adaptable to diverse organizational requirements. These features collectively contribute to building a robust, scalable, and future-proof identity management system.

The platform enhances overall system security by implementing a multi-factor authentication (MFA) mechanism grounded in three fundamental pillars of identity verification: something the user knows (such as a password or PIN), something the user has (such as a mobile device, OTP generator, or security key), and something the user is (biometric data like fingerprints or facial recognition). By requiring users to validate their identity through at least two of these factors, the system eliminates the vulnerabilities of single-factor authentication. Even in cases where passwords are compromised, unauthorized access is prevented without possession of the second factor. This layered security architecture significantly mitigates threats such as brute- force attacks, credential stuffing, and phishing scams, providing a stronger shield against evolving cyber threats.

The proposed IAM system ensures safer logins by introducing multi-step verification processes. After entering a valid password, users must complete a secondary verification step, such as entering a one-time password (OTP) sent to their registered device or approving a push notification through an authenticator application. This approach guarantees that only users who possess the verified device can complete the login process, thus preventing unauthorized access even if credentials are compromised. Such two-step confirmation mechanisms drastically reduce the risk of account takeover, thereby safeguarding both individual and organizational assets from exploitation.

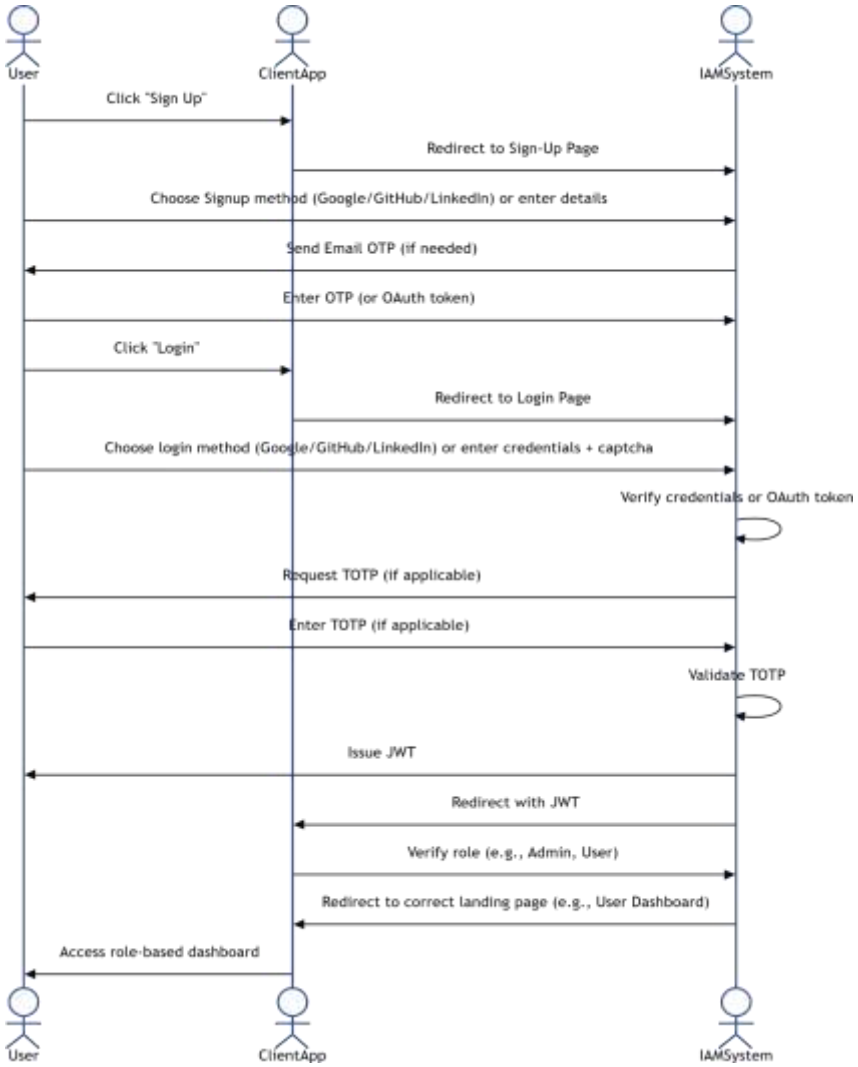
Designed with scalability in mind, the IAM platform is deployed on a cloud-native infrastructure that supports seamless growth. Whether the system is serving a startup or a global enterprise, it adapts dynamically to increasing authentication demands. Features like auto- scaling clusters automatically adjust resources based on traffic loads, ensuring consistent performance. Additionally, global edge networks enhance responsiveness for users across different geographical locations, while built-in load balancing and failover mechanisms ensure high system availability and fault tolerance. This scalable architecture allows organizations to expand their user base and integrate new services effortlessly without reengineering their authentication framework.

To provide precise and secure access control, the platform utilizes both Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC allows administrators to define roles such as “Admin,” “HR Manager,” or “Engineer,” with each role assigned a distinct set of permissions. ABAC takes this further by enforcing rules based on dynamic attributes like login time, IP address, device type, or behavioral patterns. This dual approach ensures enforcement of the least-privilege principle, allowing users access only to the data and actions necessary for their role. It also supports context-aware access policies that enhance flexibility without compromising security.

The IAM system incorporates advanced bot mitigation strategies to protect against automated threats. CAPTCHA challenges are embedded within user workflows to distinguish humansfrom bots. Additionally, device fingerprinting techniques identify suspicious or unrecognized devices attempting access, while rate limiting restricts the frequency of login or API requests to deter abuse. These mechanisms are tightly integrated into login and registration flows, providing a robust defense against threats such as credential stuffing, automated account creation, and password spraying attacks. Moreover, by blocking bot activity, the system ensures that user analytics remain accurate and infrastructure is not overloaded by illegitimate traffic.
The platform’s threat detection capabilities are powered by intelligent, real-time monitoring systems that analyze authentication activity for anomalies. Key data points include the geolocation of login attempts, frequency and patterns of failed logins, behavior across different devices or browsers, and scenarios that signal “impossible travel” (e.g., logins from widely separated locations within a short period). These insights are fed into a machine-learning-based risk scoring engine that evaluates each login attempt dynamically. Based on the risk level, the system can initiate step-up authentication measures, temporarily lock accounts, or alert administrators. This proactive threat response reduces the likelihood of attackers gaining unauthorized access and prevents lateral movement within the system.

To enable secure and efficient communication between services, the platform leverages JSON Web Tokens (JWT) and the OAuth 2.0 protocol. Rather than storing or sharing passwords, services issue signed tokens that include verified user identity, assigned roles, permissions, and token expiration details. This method facilitates seamless Single Sign-On (SSO) across multiple applications, reducing the need for users to manage multiple passwords. Moreover, each token’s scope is clearly defined, ensuring that services only access permitted data, avoiding overreach. This token-based approach not only simplifies system integration but also strengthens cross-platform security and optimizes

application performance. The proposed Identity and Access Management (IAM) platform is designed to deliver secure, scalable, and customizable user authentication and authorization services. The architecture follows a modular design, allowing easy maintenance and seamless integration with enterprise systems.



The proposed IAM platform employs a redirect-based workflow for login and signup. This workflow is designed to simplify the integration process and enhance security by eliminating the need for specific framework integrations. Here's a detailed breakdown of how the redirection process works:

Initial Request: When a user attempts to access a protected resource or performs an action that requires authentication (such as logging in or signing up), the application initiates the authentication process. The user is redirected to a secure authentication page hosted by the IAM platform.
Secure Authentication Page: The user is redirected to a secure login page managed by the IAM platform. This page is designed to handle the authentication process securely. The user enters their credentials (username and password) and, if required, additional authentication factors such as a TOTP-based OTP.

Multi-Factor Authentication (MFA): If MFA is enabled, the user will be prompted to enter a time-sensitive OTP generated by an authenticator app on their device. This adds an additional layer of security, ensuring that even if a password is compromised, unauthorized access is prevented.
Authentication Processing: The entered credentials and OTP (if applicable) are sent to the IAM platform's backend for verification. The backend uses OAuth 2.0 and JWT to authenticate the user. If

the credentials are valid, the platform generates a JWT token that represents the user's session and permissions.

Redirection to Target Page: Upon successful authentication, the user is redirected back to the target landing page from which they initiated the authentication process. This redirection is handled seamlessly by the platform, ensuring a smooth user experience. The JWT token is securely stored in the user's browser, typically in a secure cookie or local storage, to maintain the session state.

Session Management: The JWT token is used for subsequent requests to the application to verify the user's identity and permissions. The platform ensures that the token is validated for each request, maintaining the security and integrity of the user session.

Security Enhancements: The redirect-based workflow enhances security by centralizing the authentication process. By eliminating the need for specific framework integrations, the platform reduces the attack surface and simplifies the integration process. This approach also ensures that the authentication process is consistent across different applications and environments.

User Experience: The redirect-based workflow ensures a seamless user experience. Users are redirected to a secure and familiar login page, reducing the cognitive load and ensuring a consistent authentication experience. The platform's customizable authentication UIs allow organizations to personalize the login and sign-up pages to match their branding, further enhancing user experience.

III. Conclusion

The proposed Identity and Access Management (IAM) platform presents a robust, adaptable, and forward-looking solution to the challenges of user authentication and access control in modern digital environments. Unlike conventional IAM systems that often rely heavily on specific frameworks or require deep technical integration, this platform adopts a framework- agnostic architecture. This makes it significantly easier for developers to integrate it into various web and mobile applications, regardless of the underlying technology stack.

One of the key innovations is its modular and customizable design, which allows it to be embedded into diverse environments with minimal configuration. The platform prioritizes security by integrating industry-standard protocols and practices such as OAuth 2.0 for secure authorization, Multi-Factor Authentication (MFA) to prevent unauthorized access, and Role- Based Access Control (RBAC) for precise permission management. Together, these features create a multi-layered security approach that helps safeguard user data and system resources from both external threats and internal misuse.

Another standout feature of this IAM solution is its support for customizable user interfaces. Organizations can design and deploy branded login, signup, and password recovery pages that match the look and feel of their applications. This not only enhances the end-user experience but also fosters a sense of trust and continuity for users interacting with the system.

Overall, the proposed IAM platform offers a holistic solution that balances ease of integration, advanced security measures, and user-centric design—making it a valuable asset for developers and enterprises alike.

References

[1] Singh C, Warraich J, Thakkar R. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 2023;8(4):30–38. ISSN 2736-576X.

[2] Divyabharathi DN, Cholli NG. A review on identity and access management server (Keycloak). International Journal of Security, Privacy and Pervasive Computing (IJSPPC). 2020;12(3):46–53.

[3] Ding Y, Zhang Y, Qin B, Wang Q, Yang Z, Shi W. A scalable cross-chain access control and identity authentication scheme. Sensors. 2023;23(4):2000. doi:10.3390/s23042000.

[4] Alsirhani A, Ezz MM, Mostafa AM. Advanced authentication mechanisms for identity and access management in cloud computing. Computer Systems Science and Engineering. 2022;43(3):967–984.
[5] Mohammed IA. The interaction between artificial intelligence and identity and access management: an empirical study. International Journal of Creative Research Thoughts (IJCRT). 2021;9(5):668–671. ISSN 2320-2882.
[6] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control. IEEE Internet of Things Journal. 2021;8(14):11717–11731.
[7] Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials. 2019;21(2):1851–1877. doi:10.1109/COMST.2018.2866893.
[8] Zhou L, Varadharajan V, Hitchens M. Trust enhanced security architecture for cloud computing. IEEE Transactions on Information Forensics and Security. 2013;8(6):985–997. doi:10.1109/TIFS.2013.2254092.
[9] Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. Journal of Network and Computer Applications. 2014;42:120–134. doi:10.1016/j.jnca.2014.01.014.
[10] Giannetsos T, Krontiris I, Dimitriou T. Privilege escalation in IoT: The root of the problem. In: 2015 IEEE Conference on Communications and Network Security (CNS); 2015 Sep 28–30; Florence, Italy. p. 171–179. doi:10.1109/CNS.2015.7346828.