International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

KeyHound - Identity Provider and Access Management

Pratik Pawar[1], Piyush Nagarkar[2], Shreyash Hagawane[3], Saurabh Gaikwad[4], Shobha Raskar[5]

[1]Department of Computer Engineering & MESWCOE, Pune
[2]Department of Computer Engineering & MESWCOE, Pune
[3]Department of Computer Engineering & MESWCOE, Pune
[4]Department of Computer Engineering & MESWCOE, Pune
[5]Department of Computer Engineering & MESWCOE, Pune

Abstract – Single organization handles multiple applications based on different departments or needs. To access these applications, users must remember the login credentials for each. This results in the data of mutual users being stored in different identity providers, causing data redundancy and indirectly increasing storage costs. Solution is needed to globalize user credentials. Implementing a centralized system aids organizations in saving storage costs by eliminating redundant user data stored across multiple identity providers.

Key Words: Identity provider and Management, Access management, Validation, Authorization.

1. INTRODUCTION

Managing login credentials for different applications becomes challenging as the number of applications increases. From an organizational perspective, it is beneficial to have multiple applications under a single organization with distinct login credentials. The primary objective is to globalize login credentials, eliminating the need to remember multiple details. This is achieved by providing identity management on a single platform instead of using different identity providers for various applications. Consequently, data management becomes more straightforward, reducing storage requirements by minimizing data redundancy. One advantage is that users no longer need to remember numerous passwords, contributing to enhanced privacy for both users and organizations. It also upholds the integrity of users, as they are not required to save or write down credentials anywhere. Additionally, this approach offers various features, such as single sign-on, user activity monitoring, and inactive user monitoring. Moreover, there is ample room for scalability and the incorporation of additional features as needed.

2. LITERATURE SURVEY

[1]The central focus of this paper is to explore the significance of identity and access management (IAM) within information security, particularly in the context of cloud solutions. Safeguarding a system's security is a complex task, and implementing a robust IAM model is crucial for addressing security challenges, especially in cloud environments. [1]IAM as a service (IAMaaS) plays a vital role in ensuring efficient and effective access control in cloud systems, where only authorized users are granted permissions. This access control model revolves around three fundamental elements: the subject (system users requesting access), the object (the resource being accessed), and the rules that determine access approval or denial. User authentication serves as a key component in thwarting unauthorized access attempts and reducing the burden on legitimate users. It also helps prevent activities that could potentially lead to security breaches. However, one of the main challenges in implementing this IAM model lies in devising an appropriate risk assessment methodology to accurately assess and assign risk values to each access request. [1][2]This research endeavors to address this challenge by proposing a risk assessment approach that integrates IAM and Security-as-a-Service (IAMAAS) to analyze security issues and solutions within cloud services. The paper delves into the significance of Identity and Access Management (IAM) as a service in cloud environments. It highlights that digital transformation is essential for businesses, especially concerning cloud solutions. Cloud IAM services and technologies can significantly accelerate innovation and corporate development. However, security teams often face challenges in defining an appropriate cloud IAM strategy that aligns with cloud-first objectives, internal policy compliance, security, architecture constraints, and customization requirements. In summary, IAM solutions play a crucial role in ensuring cloud security through advanced authentication and permission management methods. Offering clients an up-to-date solution that automatically adjusts capacity and maintains high availability is feasible. IAMAAS also provides the advantage of not needing to run the service in the same location as the actual application, which is a significant benefit.

[2]In this groundbreaking paper, the concept of IAMaaS (Identity and Access Management as a Service) emerges as a transformative framework poised to revolutionize the landscape of cloud computing. [2]IAMaaS represents a paradigm shift in the provision of Identity and Access Management (IAM) solutions, offering cloud service providers the capability to deliver IAM functionalities directly within the public cloud environment. IAMaaS is meticulously crafted to seamlessly integrate with the core tenets of cloud computing, embodying principles of portability, scalability, and pay-per-use service. By harnessing the power of cloud infrastructure, IAMaaS transcends traditional limitations, offering unparalleled flexibility and agility to organizations seeking to fortify their digital defenses. At the heart of IAMaaS lies a sophisticated architecture, meticulously engineered to leverage the inherent capabilities of cloud computing. [2]This innovative approach is implemented using a set of virtual machines (VMs) deployed within the cloud environment, aligning seamlessly with the distributed and elastic nature of

cloud resources. By harnessing the dynamic scalability of VMs, IAMaaS ensures that organizations can effortlessly scale their identity and access management capabilities in response to evolving business needs.

[3]Identity Management (IdM) is a significant challenge in the realm of emerging scientific issues, encompassing concerns such as federation, security, and privacy. As the number of users continues to grow, Identity Management systems are constantly evolving to meet increasingly complex needs. Many existing systems require enhancements, and new solutions are also necessary to address these challenges effectively. Various Identity Management solutions are available in the market, each with its own capabilities, limitations, and adherence to specific standards and compliances. Therefore, organizations must carefully consider their specific needs and existing infrastructure when selecting an Identity Management Solution. A well-thought-out choice can not only address identity management requirements but also support security, privacy, compliance needs, and enhance user experience.

[4]In our thorough investigation, we meticulously scrutinized numerous Identity Management Systems (IMS) against a predefined set of criteria. Despite their prominence within the field, none of these systems emerged unscathed, as we uncovered deficiencies across key areas such as functionality, privacy features, and usability. To facilitate clarity and comprehension, we opted for a tabular presentation format, enabling readers to swiftly discern the nuanced strengths and weaknesses inherent in each system under evaluation. [4]Through this comprehensive analysis, we aim to catalyze discussions and innovations aimed at enhancing the efficacy and robustness of identity management solutions in the digital age.

[5]In traditional identity management paradigms, the Identity Provider (IdP) acts as a Trusted Third Party (TTP), which has significant drawbacks for both users and Service Providers (SPs). However, the emergence of blockchain-based Self-Sovereign Identity (SSI) patterns changes this dynamic by introducing a decentralized IdP and separating the identifier from identity attributes. While SSI patterns prioritize user needs, they often overlook SP requirements. This, combined with the proliferation of SSI solutions competing for user favor and the non-adherence to established protocols, poses challenges for SP adoption. To address these challenges and leverage decoupled attributes, we propose ATIB (Attribute Trust-Enhancing Identity Broker) for SPs. ATIB adopts a component-based architecture, abstracting from specific SSI solutions, enabling the issuance of verifiable claims, and employing trust models for flexible attribute-based trust decisions. We implemented ATIB as a proof of concept, integrating with uPort, Jolocom, and HL Aries/Indy.

[6]The objective of OLYMPUS is to establish a user-friendly ecosystem with privacy as a central focus. By incorporating blockchain technology, OLYMPUS aims to enhance trust across the infrastructure for users, service providers, and identity providers. This integration demonstrates that distributed identity provider technology (OLYMPUS) can be seamlessly combined with blockchain to achieve the desired level of trust. The pilot deployment and subsequent analysis suggest that there is no usability penalty for the entities involved, nor are there significant barriers hindering adoption.

The solution ensures user confidence by meticulously verifying the legitimacy of identity providers and implementing safeguards to prevent services from unilaterally altering access policies without prior notification to the infrastructure. However, several challenges surfaced during the development phase that necessitate improvements in future iterations. These challenges primarily revolve around the need to optimize cryptographic elements to accommodate resource-constrained devices, such as IoT devices, and to refine smart contracts and query methods on the blockchain platform to mitigate excessive query times as the blockchain expands. Additionally, existing blockchain-based Partially Attributed Based Credentials (P-ABC) solutions suffer from a lack of full distribution.

3. PROPOSED SYSTEM

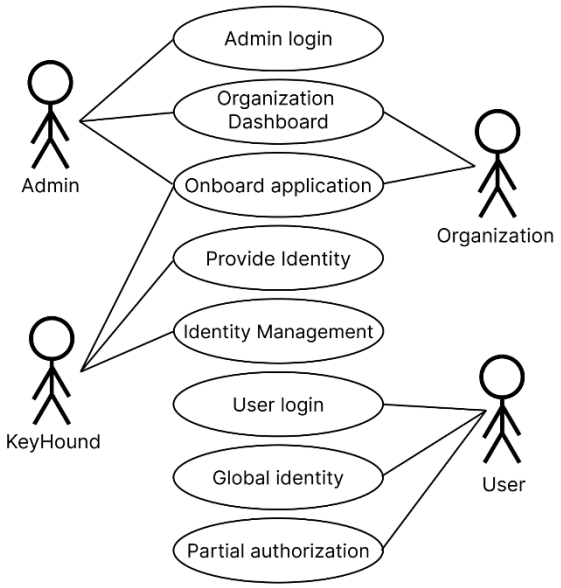

Fig -1: Figure

1. Actors:

1.1 Admin: This actor represents the system administrator responsible for managing the entire identity management system. Their functionalities likely include:

- System Configuration: Adding, removing, or modifying settings for user accounts, access levels, and security protocols within the system.
- User Management: Creating, deleting, or modifying user accounts, assigning roles and permissions, and potentially managing user groups for access control.
- Application Management: Onboarding new applications to the system, configuring user access for those applications, and potentially monitoring application activity related to user identities.
- Security Management: Implementing security best practices, managing access logs, and potentially overseeing audits and compliance with security regulations.

1.2 User: This actor represents any individual who interacts with the system to access resources or applications. Their interaction might involve:

- User Login: Providing credentials (username and password, multi-factor authentication) to authenticate and gain access to the system.
- Profile Management: Updating their own profile information within the system's limitations (depending on admin configuration).
- Password Management: Resetting forgotten passwords or potentially changing passwords based on security policies.
- Resource Access: Using the system to access authorized applications, data, or functionalities based on their assigned roles and permissions.

2. Relationships:

Association: This indicates that an actor can participate in a use case. For example, the Admin actor can perform the Admin Login use case, while the User actor can take part in the User Login use case.

Generalization (not always present): This relationship might exist if you have different types of users with varying access levels. For instance, a 'System Administrator' could be a more specific type of 'Admin' with broader control over the system.

3. Additional Considerations:

3.1 Error Handling: The diagram can be enhanced to depict potential error scenarios during login or other use cases. This could showcase how the system handles incorrect credentials, failed authentication attempts, or unexpected application integration issues.

3.2 Data Flow: If relevant, the diagram could show the flow of data between actors and the system during each use case. This clarifies how user credentials, application details, and other data are processed within the system.

3.3 Security Features: The use cases might be further detailed to highlight security best practices employed within the system. This could illustrate how password encryption, secure communication protocols, and access control mechanisms safeguard user identities and system resources.

4. CONCLUSIONS

The challenge of managing login credentials for multiple applications within an organization has been effectively addressed through the implementation of a centralized identity management system. The transition from disparate identity providers to a single platform has not only simplified user experiences but has also significantly improved organizational efficiency. By globalizing login credentials, users no longer grapple with the burden of remembering numerous passwords, leading to enhanced privacy and the preservation of user integrity. The elimination of data redundancy across multiple identity providers has not only streamlined data management but has also resulted in substantial cost savings for the organization. The introduced features, such as single sign-on, user activity monitoring, and inactive user monitoring, provide a comprehensive solution that goes beyond mere credential management.

These features contribute to a more secure environment, allowing organizations to monitor and manage user activities effectively. Additionally, the scalability of the solution ensures adaptability to evolving organizational needs, facilitating the incorporation of new features and improvements over time. In summary, the centralized identity and access management system stands as a robust solution, addressing the complexities associated with managing multiple applications and diverse user credentials. Its implementation not only fosters a more user-friendly environment but also offers significant organizational benefits, including cost savings, improved security, and adaptability to future requirements.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to Professor Shobha Raskar, our research guide, whose expertise, patience, and dedication have been invaluable. Professor Raskar's mentorship and encouragement have played a pivotal role in the successful completion of this research endeavor.

We extend special thanks to Mr. Sachin Karade, co-founder of Kondana, for his unwavering support and valuable insights that greatly enriched our research process.

We also acknowledge the support of our colleagues and peers who provided valuable insights and assistance during the course of this research.

Finally, we extend our heartfelt appreciation to all those who directly or indirectly contributed to this research project. Thank you all for your support, guidance, and encouragement.

REFERENCES

1. Ishaq Azhar Mohammed," Identity and Access Management as Security-as-Service from Clouds", Data Scientist Department of Information Technology, IJCRT, Volume 5, Issue 4 November 2017.
2. Deepak H. Sharma, Dr. C. A. Dhoteb ,Manish M. Potey," Identity and Access Management as Security-as-a-Service from Clouds", 7th International Conference on Communication, Computing and Virtualization 2016.
3. Vikas Kumar, Aashish Bhardwaj," Identity Management Systems: A Comparative Analysis", International Journal of Strategic Decision Sciences, Volume 9 • Issue 1 • January-March 2018.
4. Md. Sadek Ferdous, Ron Poet," A Comparative Analysis of Identity Management Systems", High Performance Computing and Simulation (HPCS).
5. ANDREAS GRUNER, ALEXANDER ¨MUHLE, CHRISTOPH MEINEL," Design and ¨ Evaluation of an Architecture for Brokered Self Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider", Hasso Plattner Institute (HPI), University of Potsdam, VOLUME 9, October 15 ,2021.

6. RAFAEL TORRES MORENO, JESUS´GARC´IA-RODR´IGUEZ, JORGE BERNAL BERNABE, ANTONIO SKARMETA," A Trusted Approach for Decentralised and Privacy-Preserving Identity Management", Department of Information and Communication Engineering, VOLUME 9, August 3, 2021.
7. D. Pöhn, W. Hommel: Reference Service Model Framework for Identity Management, Research Institute CODE, Universität der Bundeswehr München, 85577 Neubiberg, Germany.
8. Formal Analysis of Information Card Federated Identity-Management Protocol∗ WANG Juan1,2, HU Hongxin3, ZHAO Bo1,2, YAN Fei1,2, ZHANG Huanguo1,2 and WU Qianhong1,2, Computer School, Wuhan University, Wuhan 430072, China.
9. Self-Sovereign Identity for Organizations: Requirements for Enterprise Software RICARDO BOCHNIA, DANIEL RICHTER, AND JÜRGEN ANKE Digital Service Systems Group, HTWD – University of Applied Sciences, 01069 Dresden, Germany.
10. Hasnae L'Amrani, H., Berroukech, B. E., El Bouzekri El Idrissi, Y., & Ajhoun, R. (2016). Identity management systems: Laws of identity for models7 evaluation. 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt).
11. Zouari, J., & Hamdi, M. (2016). AIDF: An identity as a service framework for the cloud. 2016 International Symposium on Networks, Computers and Communications (ISNCC).