MZ Journals Computing Journal

Cloud identity and access management

Sandeep Reddy Gudimetla
Hindustan Computers Limited, USA
Corresponding email: sandeeprgudimetla@gmail.com

Abstract

Cloud computing has brought a new era of adaptability and scalability, which allows companies to use strong computing power and relative services. Although cloud technology has raised such security concerns as cloud identity and access management (IAM), it has become a high priority. While every organization utilizes the cloud, there are listed problems that include unsanctioned use of data, breaching of data, and culpability liabilities. Authentication systems, which are indisputably one of the most imperative aspects in the area of protection against severe threats, are one of the fields that require permanent, vigilant interaction. Solutions such as biometrics, multifactor authentications (MFA), and adaptive authentication systems are the present-day security mechanisms that make it possible to safeguard cloud resources against being accessed by malicious users.Besides this, the invention of new technologies, like deep learning and blockchain, offered a revolutionary shine to cloud identity management. AI-driven IAM solutions use AI algorithms, enabling them to study users' patterns and detect specific irregularities, providing additional protection levels through implementations that ensure enhanced security. As a result, blockchain technology has mutated and distributed trustless authentication characteristics for authorization and is most important in cloud-decentralized systems. The processes and the methods developed in this structure further improve the making of high-technology applications to avoid possible risks and support the right of organizations to utilize cloud computing.

Introduction

In the digital world that we live in, many companies are shifting towards cloud solutions for their applications, which demands IAM to be more reliable and efficient. While businesses relocate their data, applications, and services to the cloud, they encounter many security issues that are expected to be dealt with by the enriched IAM systems. This article intends to sail through the recent advancements and obstacles associated with cloud IAM systems and also, at the same time, reveal helpful strategies and approaches that can constructively bolster security in these systems.

Cloud computing as a technological phenomenon has revolutionized many industries, and any business can now get the advantage of significantly increased agility, low cost, and global accessibility. However, the new way of safety measures transforming digital banking is one of many factors in the latest security paradigms through digital transformation. There will be a re-shaping of the security paraglom, which will raise high-level security issues that include device authentication methods, access control policies, and user identity (Alsirhani et al., 2022). Also, gaining access and being equipped to pilot them is critical. With these applications, companies can fully exploit the availability and ability of their anything digital and confidential data to be protected.

Advanced Authentication Mechanisms for Cloud IAM

Recently, various research studies have concentrated on more sophisticated verification algorithms as a security matter for IAM systems in the cloud structures. This will be a drastic measure in access control, which aims to improve on the heavily deployed and user-authorization systems through the adoption of increased vetting processes as a way of developing fully protected systems from unauthorized usage or interference.

Biometrics is certainly one effort in a bigger authentication plan, which is being adopted in most countries (Alsirhani et al., 2022). Accentuating the weight of biometric authentication is biometrically based on the person's physical characteristics, such as fingerprints, iris patterns, or facial features, to confirm the identification of a person. In relation to this, each biometric system engages a unique biological and behavioral elements (Ondato, 2022), and the biometric aspects enforced on a system have an effect on performance.

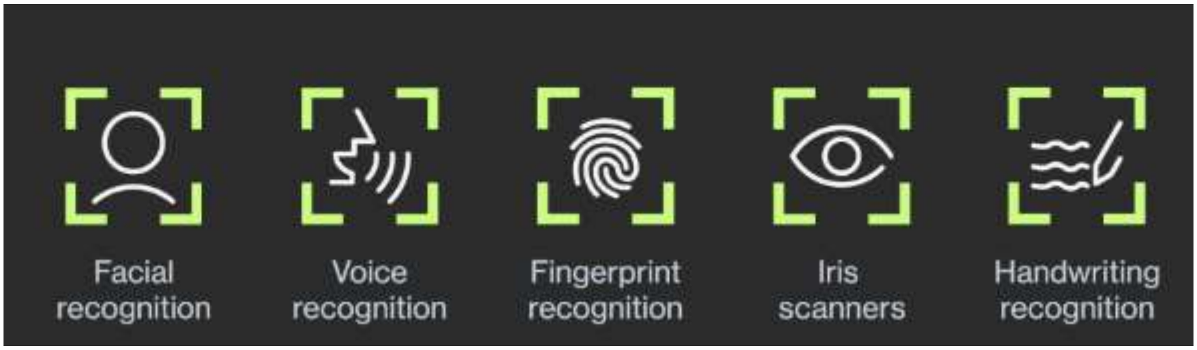

Fig. 1: Common Biometric Authentication Types (Ondato, 2022)

This approach offers a high level of security as it is inherently tied to the user's biological traits, making it difficult for unauthorized entities to gain access.

Another notable security attribute of cloud IAM is MFA in real-time (Multifactor Authentication), which has gained traction among central cloud IAM security plans. MFA revolves around verification, where the user provides different identification methods (Mohammed, 2019). Therefore, a combination of one or more factors, such as passwords, biometric profiling, or codes sent to the registered devices, is utilized.

Consequently, adaptive authentication has become integral to different Cloud IAM systems. The Adaptive Authentication process considers critical factors like the precise user location, the device type they are using, and the behavioral pattern; with this, it can assess the appropriate user access level (Mohammed, 2019). With the purpose of regular checks of every kind of multifactor authentication and changing the authentication parameters periodically, adaptive authentication is a rational approach that is in the best interests of both users in practicality and their security. With the implementation of cutting-edge authentication methods such as biometrics, MFA (two-factor authentication), and conditional authentication in the cloud, IAM is at the forefront of the rise of cloud-based identity management to cyberspace threats.

Challenges and Solutions in Cloud IAM

IAM in the cloud is becoming more complex daily, indicating a need for valuable techniques to cater to security and business process competencies described by (Indu et al., 2018; Mrabet et al., 2022). Amidst the complexities, scalability problems remain because the cloud environments have many users who increase the dimensions daily, and IAM requires help to tackle the situation. The problem of scalability, which is negative business-wise, results in users needing better network performance or a faster pace.

Consequently, their organization needs to improve its efficiency in business activities.

Interoperability is another crucial problem facing cloud authentication for multi-vendor clouds and hybrid-cloud deployments of dissimilar suppliers' technologies and platforms (Indu et al., 2018). The integration of individual, charitable, or state microfinance becomes a challenge when there are no uniform standards that make them compatible.

In addition, cloud manufacturing regulations and industry standards are another considerable issue for companies implementing IAM in the cloud. The compliance of the IAM system with the GDPR, HIPAA, and PCI-DSS regulations (among others) is a crucial consideration that the IAM process should uphold. Therefore, the development of regulatory policies should be at the top of the to-do list, as should implementing audit trails and good governance processes.

Innovative solutions like blockchain-based access control help create a decentralized ecosystem, and it is also not prone to tampering, thus increasing security and transparency (Mrabet et al., 2022). Blockchain technology guarantees the storage of identities securely, access permissions, and monitoring of audit logs in the distributed system. It also offers numerous possibilities for using them and prevents unauthorized access and data manipulations.

Through innovative approaches, these organizations can find a befitting and smooth method of addressing scalability, interoperability, and regulatory compliance. Security levels are raised, and cloud agility and efficiency are attained without creating limitations in the advanced cloud application ecosystem due to security concerns.

Conclusion

In conclusion, cloud computing has spurred the evolution of IAM to tackle emerging security challenges proactively. Implementing new IAM techniques such as biometric security, MFA, and adaptive authentication, in addition to including blockchains and AI technologies, improves cloud security. These approaches promote verification, solve problems of scalability and compliance, and make organizations work with updated cloud IAM to deal successfully with the ever-evolving cloud data protection problem.

References

Alsirhani, A., Ezz, M., & Mohamed Mostafa, A. (2022). Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. Computer Systems Science and Engineering, 43(3), 967–984. https://doi.org/10.32604/csse.2022.024854

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in a cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574–588. ScienceDirect. https://doi.org/10.1016/j.jestch.2018.05.010

Lăzăroiu, G., Andronie, M., Iatagan, M., Geamănu, M., Ștefănescu, R., & Dijmărescu, I. (2022). Deep Learning-Assisted Smart Process Planning, Robotic Wireless Sensor Networks, and Geospatial Big Data Management Algorithms in the Internet of Manufacturing Things. ISPRS International Journal of Geo-Information, 11(5), 277. https://doi.org/10.3390/ijgi11050277

Mohammed, I. A. (2019). CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL. International Journal of Innovations in Engineering Research and Technology, 6(10), 1–8. https://repo.ijiert.org/index.php/ijiert/article/view/2781

Mrabet, H., Alhomoud, A., Jemai, A., & Trentesaux, D. (2022). A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. Applied Sciences, 12(9), 4641. https://doi.org/10.3390/app12094641

Ondato. (2022). *A Complete Guide to Biometric Authentication Methods*. Retrieved from ondato.com: https://ondato.com/blog/benefits-of-biometric-authentication/