Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 2, pp. 509–519
DOI : 10.47974/JIOS-1931

Preventing insider attacks : Leveraging Identity and Access Management (IAM) solutions over traditional password-based authentication

Mallikarjun Yaramadhi *
Department of Computer Science and Engineering (Data Science)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

K. Subba Reddy †
Department of Computer Science and Engineering
Rajeev Gandhi Memorial College of Engineering and Technology
Nandyal 518501
Andhra Pradesh
India

K. Rajendra Prasad §
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

Mandavilli Kavya ‡
Department of Computer Science and Engineering (Data Science)
Malla Reddy University
Maisammaguda Dulapally
Hyderabad 500043
Telangana
India

---

* *E-mail:* **yaramadhimallikarjun@gmail.com (Corresponding Author)**
† *E-mail:* **mrsubbareddy@yahoo.com**
§ *E-mail:* **krprgm@gmail.com**
‡ *E-mail:* **kavyagudivada3@gmail.com**

© Taru Publications

Elangovan Muniyandy [@]
Department of Biosciences
Saveetha School of Engineering
Saveetha Institute of Medical and Technical Sciences
Chennai 602105
Tamil Nadu
India

S. Rajeswari [#]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Green Fields
Vaddeswaram 522302
Andhra Pradesh
India

Reeha Thouheed [$]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal 500043
Hyderabad
Telangana
India

Abstract

Advancements in web services have increased the need for enhanced security in user authentication systems. Insider attacks, where privileged insiders compromise sensitive information, pose a significant threat. Rajamanickam et al. proposed a lightweight password-based authentication using Elliptic Curve Cryptography (ECC) to prevent such attacks. However, vulnerabilities in this method were identified by Salman Shamshad et al., highlighting the need for stronger solutions. This paper advocates for Identity and Access Management (IAM) systems, which employ multi-factor authentication (MFA) and single sign-on (SSO), offering enhanced security, access control, and regulatory compliance for organizations, effectively mitigating insider threats and other cyber risks.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Authentication, Insider attacks, Elliptic curve cryptography (ECC), Identity and access management (IAM), Multi-factor authentication (MFA), Single sign-on (SSO), Vulnerabilities.*

[@] *E-mail:* **muniyandy.e@gmail.com**
[#] *E-mail:* **srajeswari@kluniversity.in**
[$] *E-mail:* **reehathouheed185581@gmail.com**

1. Introduction

The need to secure apps that link users to the internet has increased significantly with the growth of web services. One of the main components of security is authentication, which frequently asks users to give secret information to servers, like usernames and passwords, in order to verify their identities. Insider threats are among the most destructive security attacks that can target this procedure. Insider threats, in contrast to other known security assaults, include users with privileged access to the system. These users may use their credentials to break security, which could have serious and occasionally permanent repercussions. Because the attackers are trusted, insider attacks are more difficult to counter. It is crucial to create authentication systems that can withstand these attacks as a result. Elliptic Curve Cryptography (ECC) is a lightweight password-based authentication method that has been the subject of recent study by Rajamanickam et al. [1]. It is said to be resistant to known security weaknesses and insider attacks. Shamshad et al.'s study "Comments on Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC" exposed a number of flaws in the suggested ECC-based protocol, though, after more examination [2].

In this work, we conduct a critical analysis of Rajamanickam et al.'s ECC-based authentication system, emphasizing the weaknesses found by Shamshad et al. [2]. Next, as a more reliable substitute for weak password-based authentication methods, we suggest implementing Identity and Access Management (IAM) systems. Advanced authentication methods that greatly improve security and guard against insider threats are provided by IAM systems, such as single sign-on (SSO) and multi-factor authentication (MFA) [3][4].

Furthermore, more comprehensive solutions that can adjust to the increasingly sophisticated nature of threats are required given the changing cybersecurity scenario. The increasing expansion and integration of digital services by enterprises increases their vulnerability to security breaches. Therefore, it is crucial to have a multi-layered strategy to authentication and access control. Even with enhanced ECC security, traditional password-based systems might not be enough in the face of contemporary threats, when attackers use sophisticated methods like credential stuffing, phishing, and social engineering [2][5]. Shamshad et al.'s findings about the flaws in ECC-based protocols highlight the need for a paradigm change in the way authentication is handled, especially in settings where sensitive data is involved [2]. IAM solutions provide a

comprehensive security approach that goes beyond basic authentication to address these issues. They combine identity governance, access control, and ongoing monitoring to make sure that access to vital resources is strictly regulated and that unusual activity is quickly identified and addressed [6][7][8].

2. Background Information and Related Projects

2.1 *Insider Threats in Authentication Systems*

In the realm of cybersecurity, insider attacks are a serious worry, particularly in authentication systems where privileged users have access to extremely sensitive credentials. Insiders have the advantage of legitimate access, which makes it easier for them to take advantage of system weaknesses than external attackers. Conventional security measures, such intrusion detection systems and firewalls, are frequently ineffective at addressing the particular hazards posed by insiders because their primary purpose is to thwart external attacks [9][10]. Because of the implicit confidence that is put in them, these people are vulnerable to misuse, which can result in harmful activity [11] that can be challenging to identify and stop, unauthorized access, or data breaches [12]. More advanced authentication methods that go beyond simple password protection are urgently needed, given the potential for serious harm. These cutting-edge technologies, including multi-factor authentication (MFA) and continuous monitoring, are crucial for reducing the dangers brought on by insider threats by making sure that access to critical data is strictly regulated and that any questionable activity is quickly discovered [13].

2.2 *Elliptic Curve Cryptography (ECC) in Authentication*

This method provides a quick and safe authentication process by utilizing the cryptographic powers of ECC. Nevertheless, despite these encouraging features, more research has cast doubt on the system's ability to completely thwart insider threats by pointing out potential weaknesses that could be exploited. This has raised questions about the system's overall dependability in situations involving critical security.

2.3 *Identity and Access Management (IAM) Solutions*

Solutions for Identity and Access Management (IAM) provide a strong foundation for controlling user identities and granting access to important resources inside a company. These systems incorporate

sophisticated techniques like Single Sign-On (SSO) and Multi-Factor Authentication (MFA), which greatly enhance security, going beyond the conventional password-based authentication. While SSO simplifies access across different platforms with a single set of credentials, lowering the risk of password fatigue and related vulnerabilities, MFA strengthens protection by requiring multiple kinds of authentication.

3. Analysis of ECC-Based Authentication

3.1 *Evaluation of Rajamanickam et al.'s ECC-Based Protocol*

An ECC-based authentication system was created by Rajamanickam et al. with the intention of addressing a number of security flaws, including insider threats. To secure communication between clients and servers, the protocol makes use of Elliptic Curve Cryptography's (ECC) strong cryptography. But further investigation by Shamshad et al. found serious flaws in the protocol, especially in the client-server authentication procedure. Insiders may be able to take advantage of these flaws to obtain illegal access and jeopardize the security of the system as a whole. The results indicate that even with ECC's robust cryptographic base, the protocol would not be completely immune to insider assaults, underscoring the need for more development and thought-out security precautions.

3.2 *Vulnerabilities in the Client-Server Authentication Process*

The vulnerabilities found by Shamshad et al. [2] reveal serious weaknesses in the ECC-based protocol's authentication procedure, raising serious questions about how well it protects against insider attacks. Insiders who already have some degree of access may be able to circumvent authentication procedures and enter restricted regions of the system without authorization thanks to these vulnerabilities. Once inside, the integrity and security of the system could be jeopardized since they might access, change, or even remove important data. The potential for such manipulations not only jeopardizes data availability and confidentiality, but it also erodes confidence in the security protocols meant to guard against these very dangers. The identification of these flaws raises concerns about the ECC-based protocol's overall resilience and raises the possibility that, despite its excellent cryptographic security, insider assaults may still be possible. This emphasizes the requirement for more thorough security measures that target insider risks in particular.

4. The proposed Insider Threat Protection Method Based on IAM

4.1 *Advantages of IAM Solutions*

Because Identity and Access Management (IAM) solutions integrate advanced security elements that give greater protection, they enable significant enhancements over standard password-based authentication systems. The use of multi-factor authentication is one of the main benefits (MFA). Before allowing access, MFA requires users to submit many types of authentication, such as a password, a biometric scan, or a one-time code given to a mobile device. Because it ensures that unauthorized access is extremely difficult, even in the event of one element being compromised, this layered method greatly increases security. IAM systems significantly reduce the likelihood that insiders will be able to use guesswork or stolen credentials by implementing MFA. SSO, which streamlines the user's experience by enabling the access to apps with a single set of credentials, is another important advantage of IAM systems. Because of this convenience, users are less likely to turn to weak or simple passwords when they become fatigued with their passwords. In addition to improving usability, SSO centralizes authentication, which facilitates the enforcement of uniform security standards by enterprises across many platforms. By taking a more simplified approach, the security risks related to password management are reduced, and a stronger overall security posture is maintained. IAM solutions also provide more efficient monitoring and response to possible security concerns by centrally managing user identities and access controls. Organizations may more easily track and audit user actions, identify anomalies, and enforce access regulations by

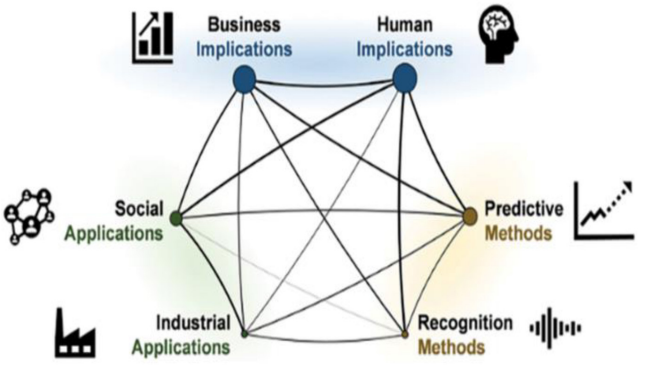


Figure 1

Identity and Access Management (IAM) solutions

combining identity management into a single solution. The use of centralized oversight enhances the capacity to detect and address questionable conduct, thereby mitigating the likelihood of insider threats and guaranteeing stringent control over access to confidential data. All things considered, IAM solutions provide a thorough method of handling security, mitigating the drawbacks of conventional password-based systems and offering improved defense against a range of threats. Figure 1 shows the IAM solution.

4.2 *Implementation of IAM Solutions*

As shown in Figure 2, authentication techniques and access controls must be strategically integrated into the current security architecture in order to implement Identity and Access Management (IAM) systems. Multi-Factor Authentication (MFA) is usually implemented first, adding additional layers of verification to the authentication process. Users using MFA must submit extra forms of identity in addition to their typical password, like a biometric scan or a one-time passcode. This action improves security considerably by making it more difficult for unauthorized users to have access, even in the event that they manage to get the essential credentials.

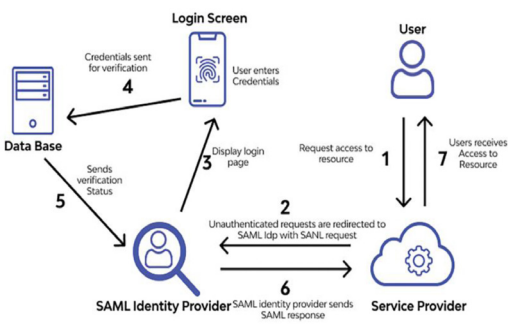


Figure 2

Implementation of Identity and Access Management (IAM) solutions

4.3 *Mitigating Insider Threats with IAM*

The Identity and Access Management (IAM) solutions, with their sophisticated authentication procedures and the strict access controls, are essential for reducing insider threats. The Multi-Factor Authentication (MFA), where the users are required to submit various forms of verification, such as a password, a biometric scan, or a one-time code, is one of the

main aspects of Identity and Access Management (IAM) systems. This extra security measure greatly lessens the possibility that insiders may use their credentials for nefarious purposes. The additional authentication measures act as a barrier, making illegal access more difficult, even in the event that an insider's password is compromised.

Security Level with IAM Solutions (2019–2023)

The security levels attained over the previous five years with IAM (Identity and Access Management) technologies are shown figure 3. Security is expected to rise steadily, from 60% in 2019 to 95% in 2023, according to the trend. This suggests that modern authentication technologies like SSO and MFA, which successfully reduce the risks of insider threats and illegal access, have been gradually included to IAM solutions to increase security.

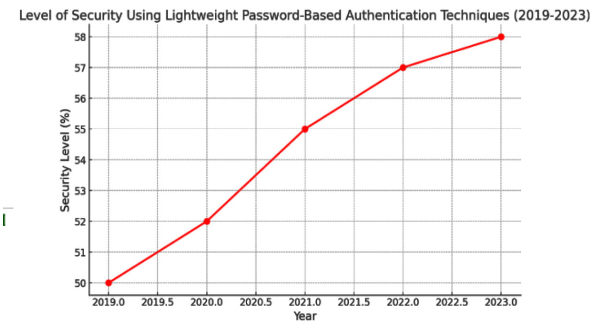


Figure 3

Security Level using Lightweight Password

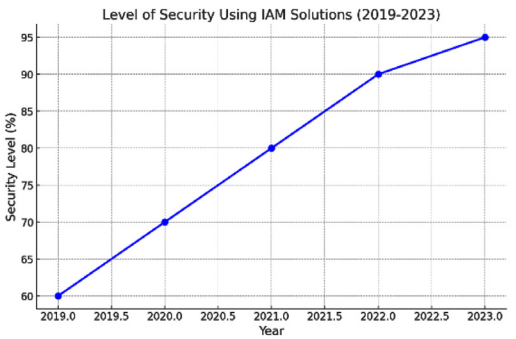


Figure 4

Security Level using IAM

Security Level with IAM Solutions (2019–2023)

The security levels attained over the previous five years with IAM (Identity and Access Management) technologies are shown in figure 4. Security is expected to rise steadily, from 60% in 2019 to 95% in 2023, according to the trend. This suggests that modern authentication technologies like SSO and MFA, which successfully reduce the risks of insider threats and illegal access, have been gradually included to IAM solutions to increase security.

IAM Solutions vs. Lightweight Password-Based Authentication: A Comparison of Security Levels (2019–2023)

Figure 5 shows how, over the previous five years, the security levels of IAM systems and Lightweight Password-Based Authentication Techniques have differed. The comparison demonstrates the distinct security advantage of IAM solutions, which often beat the conventional password-based method. Although both approaches have improved, IAM systems have achieved much higher security standards, proving that they are capable of offering strong defense against ever changing security threats.

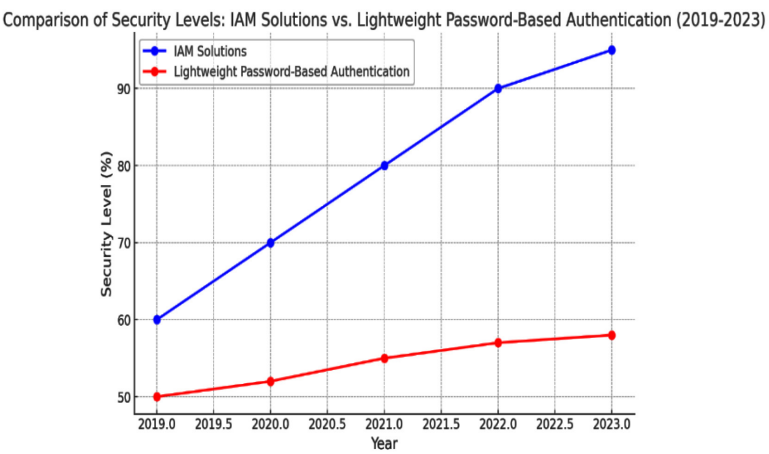


Figure 5

Comparison

5. Discussion and Conclusion

The strength of the existing authentication procedures has a major impact on the security of web services. Lightweight password-based

authentication methods provide some security, but they might not be enough to fend against insider attacks. One such method is the ECC-based protocol put forth by Rajamanickam et al. The flaws that Shamshad et al. found highlight the necessity of a more thorough approach to authentication. IAM systems offer a more potent defence against insider threats because to their sophisticated authentication procedures and centralized access management. Organizations can improve the security of their web services, safeguard confidential data, and guarantee regulatory compliance by putting IAM solutions into place. In summary, the use of IAM systems offers a more reliable and scalable method of preventing insider threats, even while ECC-based authentication has some benefits of its own. In order to build a more robust security framework for online services, future research should concentrate on improving IAM technologies even further and investigating how they might be integrated with other cutting-edge security paradigms.

References

[1] S. Rajamanickam, S. Vollala, R. Amin, and N. Ramasubramanian, "Insider attack protection: Lightweight password-based authentication techniques using ECC," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1972–1983 (2019).

[2] S. Shamshad, K. Mahmood, S. Kumari, and M. K. Khan, "Comments on 'Insider attack protection: Lightweight password-based authentication techniques using ECC'," *IEEE Systems Journal*, vol. 15, no. 1, pp. 877–880 (2020).

[3] M. A. Thakur and R. Gaikwad, "User identity and access management trends in IT infrastructure—An overview," in *Proc. 2015 Int. Conf. Pervasive Comput. (ICPC)*, Pune, India, pp. 1–4 (2015). doi: 10.1109/PERVASIVE.2015.7086987.

[4] Y. Yang, X. Chen, G. Wang, and L. Cao, "An identity and access management architecture in cloud," in *Proc. 2014 7th Int. Symp. Computational Intelligence and Design*, vol. 2, Hangzhou, China, pp. 200–203 (2014). doi: 10.1109/ISCID.2014.211.

[5] V. Singh, P. Dahiya, and S. Singh, "Smart card-based password authentication and user anonymity scheme using ECC and steganography," in *Proc. 2014 Int. Conf. Advances in Computing, Communications and Informatics (ICACCI)*, Delhi, India, pp. 1614–1621 (2014). doi: 10.1109/ICACCI.2014.6968516.

[6] Indu and P. M. R. Anand, "Identity and access management for cloud web services," in *Proc. 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, Trivandrum, India, pp. 406–410 (2015). doi: 10.1109/RAICS.2015.7488432.

[7] J. Petrovska, A. Memeti, and F. Imeri, "SOA approach—Identity and access management for the risk management platform," in *Proc. 2019 8th Mediterranean Conf. Embedded Computing (MECO)*, Budva, Montenegro, pp. 1–4 (2019). doi: 10.1109/MECO.2019.8760185.

[8] B. Li, G. Zhang, S. Lei, H. Fu, and J. Wang, "A lightweight authentication and key agreement protocol for IoT based on ECC," in *Proc. 2021 Int. Conf. Advanced Computing and Endogenous Security*, Chengdu, China, pp. 1–5 (2022). doi: 10.1109/ICACES53779.2022.9763954.

[9] W. R. Claycomb, C. L. Huth, B. Phillips, L. Flynn, and D. McIntire, "Identifying indicators of insider threats: Insider IT sabotage," in *Proc. 2013 47th Int. Carnahan Conf. Security Technology (ICCST)*, Medellín, Colombia, pp. 1–5 (2013). doi: 10.1109/CCST.2013.6922066.

[10] E. N. Yılmaz, B. Ciylan, S. Gönen, E. Sindiren, and G. Karacayılmaz, "Cybersecurity in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect," in *Proc. 2018 6th Int. Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, Istanbul, Turkey, pp. 81–85 (2018). doi: 10.1109/SGCF.2018.8408941.

[11] Y. G. Wu, W. H. Yan, and J. Z. Wang, "Real identity-based access control technology under zero trust architecture," in *Proc. 2021 Int. Conf. Wireless Communications and Smart Grid (ICWCSG)*, Shenzhen, China, pp. 18–22 (2021). doi: 10.1109/ICWCSG53441.2021.9698374.

[12] K. S. Reddy, K. R. Prasad, G. R. Kamatam, R. S. Sharma, P. V. Rao, and N. K. Gupta, "An extended visual method to perform data cluster assessment in distributed data systems," *J. Supercomput.*, vol. 78, pp. 8810–8829 (2022), doi: 10.1007/s11227-021-04243-z.

[13] K. N. Kumar, C. K. Mohan, and L. R. Cenkeramaddi, "The impact of adversarial attacks on federated learning: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.* (2023). doi: 10.1109/TPAMI.2023.3322785.

Received November, 2024