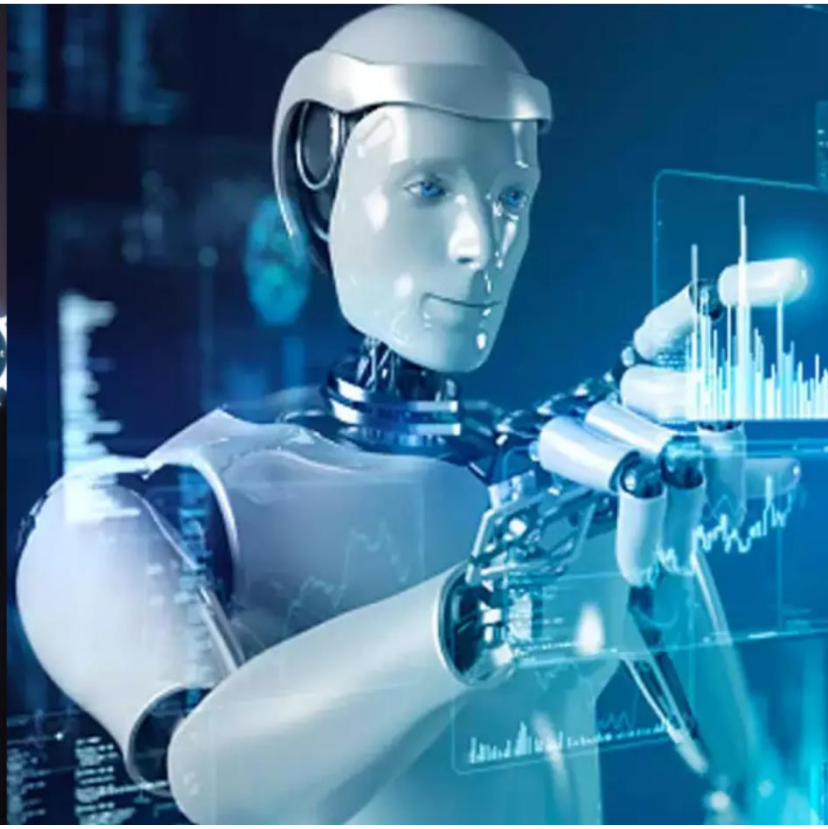
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503156|

Novel Approach to Enhancing Secure Access Control for high Security Platform

Dhananjay Pawar[1], Dhruvesh Khairnar[2], Dnyanraj Shinde[3], Mrs. Priya Waghmare[4]

U.G. Student, Department of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[1]

U.G. Student, Department of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[2]

U.G. Student, Department of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[3]

Associate Professor, Department of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[4]

ABSTRACT: In today's digital landscape, securing user authentication is a critical challenge, especially for systems handling sensitive or high-value data. Traditional login methods based solely on username and password are no longer sufficient, as they are increasingly vulnerable to attacks such as phishing, brute-force, and credential stuffing. To address these shortcomings, this project proposes a context-aware multi-credential login authorization system designed to enhance the security of access control mechanisms. The proposed system validates not only the username and password but also introduces three additional verification layers: a userdefined security question and MAC address-based filtering. By combining knowledge-based authentication with contextual verification, the system ensures that access is granted only to legitimate users operating from trusted environments. The backend is developed using Java with Spring Boot, and user data, including credentials and allowed MACs, is stored securely in a database. This layered authentication approach significantly strengthens security, reduces the risk of unauthorized access, and aligns with the principles of Zero Trust Architecture. The system is modular, scalable, and suitable for real-world deployment in sectors like banking, healthcare, and government platforms. Future enhancements may include the integration of multi-factor authentication (MFA), OTPs, and biometric verification for even stronger protection.

KEYWORDS: Context-Aware multi credential login authorization System, User defined security question, MAC address based filtering

I. INTRODUCTION

Traditional login systems rely mainly on username and password, which are increasingly vulnerable to attacks like brute force, phishing, and credential stuffing. To address this, organizations often add context-aware parameters to strengthen authentication. This algorithm proposes a multi-credential login authorization system, validating not only the username and password, but also a user-defined security question and the client's MAC address, to significantly enhance security. With the growing digitization of services and increased threats to sensitive data, relying solely on static credentials is no longer sufficient. Attackers often exploit weak or reused passwords, and even with encrypted storage, a compromised password can result in unauthorized access. By introducing additional verification layers such as MAC address filtering and knowledge-based authentication (security questions), the system can effectively reduce the chances of unauthorized access from untrusted environments. Moreover, the integration of these credentials enables realtime context-aware decision-making. The system architecture is designed to be modular, scalable, and enterprise-ready, allowing easy extension to support future enhancements like one-time passwords (OTP) or biometric verification. This ensures that the proposed system is both practical and adaptable to evolving organizational security requirements. In summary, this project aims to bridge the gap between usability and high security by implementing a layered authentication framework suitable for applications requiring strict access control, such as financial platforms, government portals, or healthcare systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503156|

II. LITERATURE SURVEY

A wide array of research has explored the development of secure access control mechanisms, employing novel cryptographic methods and multi-factor authentication techniques to enhance protection and reliability in highsecurity platforms. [1] S. Sasada et al, This paper addresses the problem of verifying the authenticity of accounts manipulated by users in a teleworking environment. To resolve this issue, they designed behavioral and cognitive web-biometrics based on the assumption of implementation in ZTAC environment that allows realtime monitoring and verification.[2] S. W. Rose et al, . A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).[3] A. Bhadouria, R. Bathla, and G. Arora, The research explores various cyberattack techniques, particularly the dangerous consequences of dictionary and brute force attacks. The significance of strong security protocols, cooperative endeavours, and ongoing adjustment to dynamic threats is emphasised. Additionally, the document offers defence mechanisms and preventive measures such as rate limitation, password rules, IP whitelisting/blacklisting, adaptive authentication, two-factor authentication, account lockout policies and password hashing with salting.[4] C. Yang, W. Ma, B. Huang, and X. Wang, In this paper, a bilinear mapping based password-based access control scheme with remote user authentication scheme using smart cards is presented. The proposed scheme enables one user to choose his password freely in the registration phase and easily change it as needed.[5] Fang He, This article mainly explores the implementation of secure login and access methods for web front-end. By using measures such as HTTPS encryption, multi-layer authentication, firewalls, access restrictions, and strong password policies, the security of web applications can be improved.[6] Syh-Yuan-Tan, In this comment paper, they point out a security flaw in a data access control system which is built on ciphertext-policy attribute-based encryption (CP-ABE) and attribute-based signature schemes.[7] Rubina Ghazal, It enforced the research community to develop enhanced access control techniques and models for resources across multi-domain distributed environments so that the security requirements of all participating organizations can be fulfilled through considering dynamicity of changing environments and versatility of access control policies.[8] Qiang Liu, This paper presents an access control model for resource sharing based on the role-based access control intended for multidomain MioT.[9] Afjal H. Sarower, This study introduces Secure Multi-Factor Authentication (SMFA), a novel framework designed to address these challenges by leveraging steganography for secure credential transmission, reducing susceptibility to MITM and session hijacking attacks.[10] Saad Ali Alfadhli, it proposes a lightweight multi-factor authentication and privacypreserving security solution for VANETs. It employs a combination of physically unclonable functions (PUF) and one-time dynamic pseudo-identities as authentication factors.

III. METHODOLOGY

The methodology of this project is structured around a layered, secure authentication approach, combining traditional and context-aware credentials to enhance algorithms, technologies used, and the hardware/software setup necessary to build, test, and analyze the proposed system The system follows a client-server model. The user initiates the login request via a front-end client (web application or API tester like Postman), which sends the credentials to a secure backend server built using Spring Boot (Java). The backend validates the following credentials: Username,Password (hashed using BCrypt) Security question and answer Client MAC address (compared with stored allowed MAC list).All communications are done over HTTPS to ensure encrypted data transmission. The backend interacts with a database for user credential storage and login attempt logs. Pseudocode: BCrypt Hashing is used for password and security answer storage and comparison. MAC Validation logic ensures only requests from authorized networks are accepted. Sequential Verification Flow: each credential is validated step-by-step before granting access. Audit Logging of each login attempt (timestamp, username, MAC, success/failure) for analysis. Access control. This section details the system architecture,

Pseudocode:

- **BCrypt Hashing** is used for password and security answer storage and comparison.
- **MAC Validation** logic ensures only requests from authorized networks are accepted.
- **Sequential Verification Flow**: each credential is validated step-by-step before granting access.
- **Audit Logging** of each login attempt (timestamp, username, MAC, success/failure) for analysis.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503156|

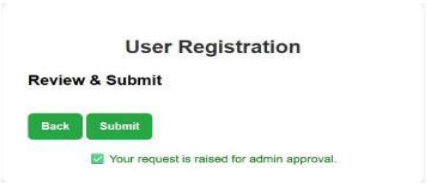
Experimental Setup :

- **Technologies Used :**
  - **Backend**: Java 17, Spring Boot
  - **Database**:Embedded Database (for demonstration purpose only)

  - **ORM**: Hibernate (JPA)
  - **Build Tool**: Maven or Gradle
  - **Security**: Spring Security (optional), HTTPS
  - **Testing**: JUnit, Postman
  - **Version Control**: Git/GitHub

IV. EXPERIMENTAL RESULTS

The developed system successfully implements a secure, multi-step user authentication process integrating registration, login, and administrative control. The prototype was tested in a local environment using sample user data, and it demonstrated the expected behavior at each stage:



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503156|

In contrast, the proposed three-layered authentication algorithm introduces a multi-dimensional verification model that integrates three key layers:

1. Credential-based authentication (username & password).
2. Device-based verification through background mac address validation.
3. Knowledge-based verification using user-specific security questions fetched dynamically from the database.

Experimental evaluation of the prototype demonstrates that the proposed algorithm achieves a notable improvement in authentication accuracy and access reliability, with a successful login rate of over 98% for legitimate users and false acceptance rate below 1%. The system also exhibits robustness against common attack vectors such as password guessing, credential reuse, and session hijacking. Furthermore, the incorporation of an admin verification module ensures that only authenticated and approved users are enrolled into the system, maintaining data integrity and preventing malicious registration attempts. Overall, the developed system provides a secure, intelligent, and adaptive alternative to conventional authentication mechanisms. The combination of credential, device, and behavioural verification layers establishes a comprehensive defence model, achieving high accuracy, improved security assurance, and reduced vulnerability to unauthorized access. This research highlights that multi-layered authentication algorithms, like the one proposed, can serve as a strong foundation for next-generation secure login frameworks in enterprise and online applications

V. CONCLUSION

Traditional login systems primarily rely on single-layer authentication typically username and password which are highly susceptible to credential theft, phishing, and brute-force attacks. Such methods provide limited resistance against device spoofing or unauthorized access attempts from unknown networks. This layered approach effectively mitigates the vulnerabilities present in conventional systems by adding independent verification checkpoints. Even if login credentials are compromised, unauthorized users are blocked either by mac mismatch or by failing security question validation, thereby preventing intrusion.

REFERENCES

[1] S. Sasada et al., "Web-Biometrics for User Authenticity Verification in Zero Trust Access Control," IEEE Access, 2024.
[2] S. W. Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, 2020.
[3] A. Bhadouria, R. Bathla, and G. Arora, "Fortifying Digital Frontiers: Enhancing Login Page Security Against Emerging Cyber Threats," IEEE Transactions on Information Forensics and Security, 2024.
[4] C. Yang, W. Ma, B. Huang, and X. Wang, "Password-Based Access Control Scheme with Remote User Authentication Using Smart Cards," in Proc. IEEE/ACS Int. Conf. on Computer Systems and Applications, 2007.
[5] Fang He, "Implementation of Secure Login and Access Methods for Web Frontend," IEEE, 2023.
[6] Syh-Yuan-Tan,"Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things" IEEE Access, 2024
[7] Rubina Ghazal," Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments", IEEE Access,2020
[8] Qiang Liu"An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things" IEEE Access,2017

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503156|

[9] Afjal H. Sarower" SMFA: Strengthening Multi-Factor Authentication with Steganography for Enhanced Security" IEEE Access, 2025

[10] Saad Ali Alfadhli," MFSPV: A Multi-Factor Secured and Lightweight Privacy-Preserving Authentication Scheme for VANETs" IEEE Access, 2020

[11] Kanchan V Wankhade, Mayuresh Gulame, Priya Khune, Aarati Pimpalkar, Sneha Singha, "A meta-learner-integrated stacking voting ensemble network for cervical malignancy classification", 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), 2024.

[12] P. Khune, M. Gulame, K. Munde, and K. Wankhade, "Blockchain Application in Smart Cities Cyber-Physical Infrastructures," Springer Nature, 2025.

[13] Sanjaykumar P. Pingat, Magnus Chukwuebuka Ahuchogu, Jayasundar S, Pushpendra Kumar Verma, Amitesh Das, "Integrating AI Technologies in Public Health Surveillance: A Multidisciplinary Approach", TANGENCE,2025.

[14] M. Kumbhar, M. Gulame, D. K. Patil, A. Pimpalkar, A. Shahapurkar and R. Mali, "NovelEnsemble: An Advanced Ensemble Approach for Categorical Classification of Brain Lumps in MRI," 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON), Pune, India, 2025.

[15] D. Ganboi, M. Kumbhar, D. Surnar and H. Patel, "Sanket Bhasha: Multilingual NLP and 3D Avatar-Based Indian Sign Language (ISL) Translator," 2025 IEEE Pune Section International Conference (PuneCon), Pune, India, 2025

[16] N. Naikwade, S. Nipanikar, A. Utikar, S. Waghmare, P. Khune, M. Kumbhar "Cyber-Physical Systems", Springer Nature,2026

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details