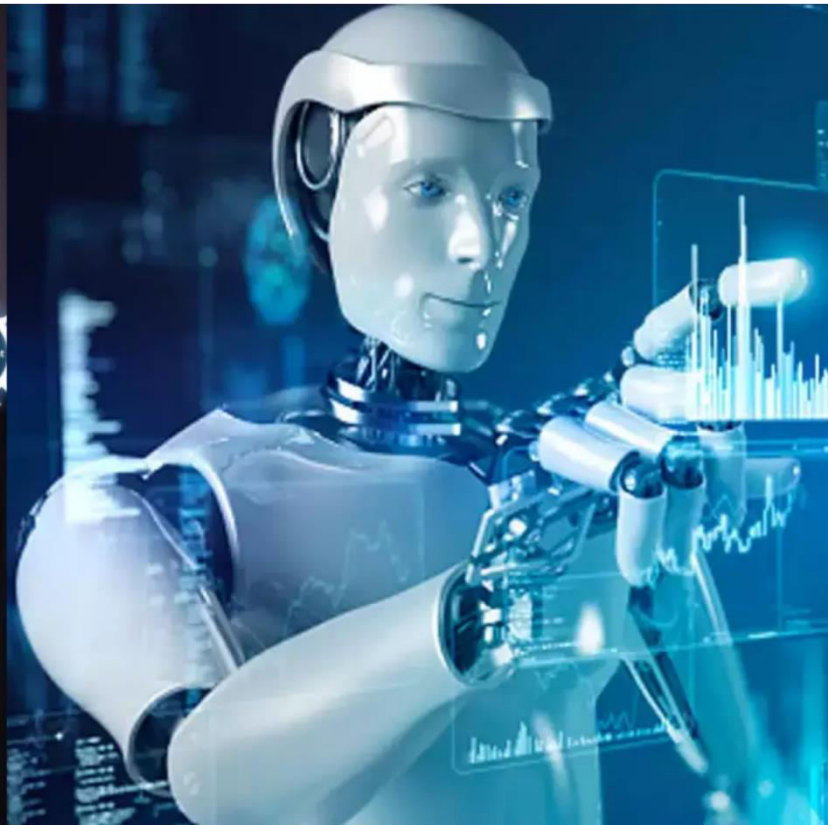
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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.2026.1503368|

Intelligent Login Security with Fake Trap Protection

Nithisha M[1], Padmavathi M G[2], Ashmi A J[3], Mrs. Sajitha M S[4]

Student, Department of Information Technology, Arunachala College of Engineering for Women, Nagercoil, Tamil Nadu, India [1,2,3]

Assistant Professor, Department of Information Technology, Arunachala College of Engineering for Women, , Nagercoil, Tamil Nadu, India [4]

ABSTRACT: Due to flaws in conventional password-based techniques, user authentication security has become crucial with the growing reliance on digital systems. A multi-layered authentication system with detection and deception techniques is presented in this project, "Intelligent Login Security with Fake Trap Protection." In order to calculate an accuracy score, the system verifies the MAC address, IP address, location, and time zone following login. Access is provided with a device-linked secure number as a supplementary layer, permitting only two attempts, if the score is ≥80%. Users are redirected to a honeypot portal in the event of failure. Users are taken straight to the fraudulent site and have to complete OTP verification if the score is less than 80%. During this time, the account is temporarily disabled. The administrator receives verified information for monitoring and additional research.

KEYWORDS: Intrusion Detection Systems (IDS), OTP Verification, Time Zone Validation, MAC Address Verification, IP Address Tracking, Multi-factor Authentication (MFA), User Authentication Security, Deception Technology, Fake Login Portal Detection, Risk-based Authentication.

I. INTRODUCTION

Online authentication solutions are essential for protecting data storage, transmission, and access control in the digital age. Users are depending more and more on digital systems for tasks like banking, e-commerce, and data exchange due to the quick expansion of web applications and cloud platforms. But because of this reliance, there are now more cyberthreats, such as phishing, credential theft, and illegal access. Because weak or reused credentials can be readily abused using brute-force attacks and social engineering tactics, traditional authentication solutions that rely just on usernames and passwords are extremely susceptible.

By adding sophisticated verification procedures, contemporary authentication systems are moving beyond static credentials to overcome these issues. The "Intelligent Login Security with Fake Trap Protection" project suggests a multi-layered authentication system that integrates device and environmental analysis with credential validation. Following login, the system assesses the user's validity based on factors including MAC address, IP address, location, and time zone. When these attributes do not match the registered profile, access can be denied even if credentials are hacked, enhancing security.

This system's deception-based protection mechanism is one of its main contributions. When a login attempt is deemed suspicious due to mismatched parameters or low prediction scores, it is sent to a phony portal that imitates the actual system. This method lets managers keep an eye on invader behavior while preventing hackers from obtaining private information. After being redirected to a secure site, legitimate users must complete an extra device-linked verification. The system offers a proactive and adaptable security approach that improves data protection and resistance against cyberattacks by combining intelligence analysis, multi-factor verification, and deception tactics.

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.2026.1503368|

II. PROBLEM STATEMENT

Authentication systems are now a prominent target for cyberattacks due to the quick expansion of internet platforms. Conventional techniques that depend on usernames and passwords are susceptible to credential theft, phishing, and brute-force attacks, which enable hackers to gain unauthorized access to systems.

These systems are vulnerable to unwanted access because they lack intelligent verification of device and environmental characteristics including MAC address, IP address, location, and time zone. They also lack real-time alerts for administrators and deception capabilities to identify or mislead invaders. Using multi-layered authentication, device validation, and login scoring, this project suggests an Intelligent Login Security solution with Fake Trap Protection. Administrator alerts facilitate efficient monitoring and security, while suspicious users are sent to a phony portal.

III. LITERATURE SURVEY

Ensuring safe user authentication has grown to be a significant cybersecurity concern due to the quick expansion of web-based applications. Conventional authentication techniques that rely solely on usernames and passwords are extremely susceptible to threats like phishing, brute-force assaults, and credential theft. One-Time Passwords (OTP) and email verification are examples of Multi-Factor Authentication (MFA) procedures that have been established to increase security.

Current methods concentrate on context-aware authentication, which uses contextual factors like IP address, MAC address, location, and time zone to confirm user identity. These techniques aid in determining whether an attempt to log in is coming from a known or unknown environment.

Additionally, in order to track and trap attackers without disclosing actual data, deception-based security measures like phony login portals are employed. By incorporating environment-based verification and fake trap methods to improve login security, the suggested system expands on these strategies.

IV. PROPOSED METHODOLOGY AND DISCUSSION

The proposed system is by implementing a multi-layered security architecture, the suggested system—named Intelligent Login Security with Fake Trap Protection—is intended to get around the drawbacks of conventional authentication methods. This system incorporates environmental verification and deception tactics to improve security and stop unwanted access, in contrast to traditional approaches that solely use usernames and passwords. The user inputs their registered email address and password during the system's initial authentication process. To guarantee accuracy, these credentials are checked against the database. In order to prevent unauthorized users from directly accessing further stages, the system only moves on to the next step of verification when the credentials match.

This system collects environmental data, including MAC address, IP address, location, and time zone, after the main authentication is completed. These parameters are contrasted with the user's previously saved data. By doing this step, you can be sure that the login attempt is coming from a known and reliable source. Based on the gathered environmental data, a prediction method is then used to determine a similarity score. The system regards the user as valid if the score is at least 80%, which is the established level. If not, the attempt to log in is marked as suspicious, and the proper action is taken.

Using safe number verification, the system adds an extra security layer for authorized users. The user must input a security number that is exclusive to their device. The user can access the main system if they enter the correct security number. The user is taken to a phony portal if the number of incorrect tries exceeds the limit.

The system initiates the false trap mechanism in response to suspicious users or unsuccessful verification attempts. The user is taken to a phony portal that mimics the original interface but does not provide them access to actual data. This strategy aids in deceiving adversaries while shielding the system from harm.

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.2026.1503368|

Finally, the system's methodology incorporates admin notification and OTP verification. The account is temporarily banned until validation is finished, and an OTP is issued to the user's registered email for further verification. The system simultaneously transmits information to the administrator for monitoring and additional action, including IP address, MAC address, location, and time zone.

V. SYSTEM ARCHITECTURE

The Intelligent Login Security with Fake Trap Protection system architecture establishes a structured framework that unifies several security layers, data validation techniques, and user interaction modules. It shows how various parts interact and handle information to guarantee that authorized users are given safe access while unauthorized users are recognized and sent to a restricted fictitious environment.

By combining conventional authentication techniques like email and passwords with environment-based verification, secure number validation, and fake trap mechanisms, the architecture aims to improve system security and intelligence. The system is a proactive and flexible security solution since it also allows for administrator notice and real-time monitoring.

Users can interact with the application through the User Interface Layer, which serves as the system's entry point. It consists of the fake trap portal, security verification interface, and login page. Users are dynamically redirected to either the secure system or the fictitious site intended for questionable actions, depending on the authentication result.

The system's primary processing and logic are handled by the application layer. It consists of a variety of interrelated modules, including admin alert production, OTP verification, prediction algorithms, secure number validation, false trap mechanisms, environmental verification, and login authentication. Together, these modules calculate trust scores, verify user identities, and effectively manage access flow.

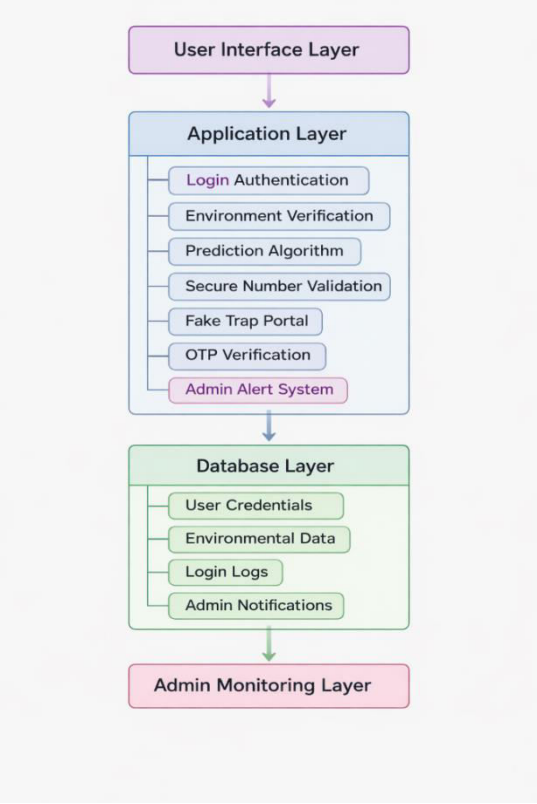


Figure 1.1 System Architecture

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.2026.1503368|

All of the crucial information needed for monitoring and authentication is managed and stored by the database layer. It keeps track of login logs, admin notification records, secure numbers, environmental parameters, and user credentials. During system operations, this guarantees dependable data storage and retrieval.

Sensitive data is protected by the Security Layer using access control, validation, and encryption techniques. By employing secure number validation and environmental similarities to authenticate user identification, it prevents unwanted access. It also uses fake portal deception to protect actual system data.

Finally, real-time visibility into system activity is offered via the Admin Monitoring Layer. Administrators may track suspicious activity, keep an eye on login attempts, and get comprehensive notifications with details like IP address, MAC address, location, and time zone. This makes it possible to respond quickly and manage threats effectively.

Workflow of the System Architecture

Users logs in using their email address and password, which are then compared to their saved credentials, to start the system procedure. Environmental factors such MAC address; IP address, location, and time zone are gathered and compared with previously saved user data upon successful authentication.

The validity of the login attempt is then assessed using a prediction score. The user moves on to secure number verification if the score is 80% or greater, and access to the main portal is then allowed after successful entry. The system marks an attempt as suspicious if the score is below the cutoff or if the secure number is repeatedly entered incorrectly. The administrator is informed while activities are recorded, the user is taken to a phony portal, and an OTP is sent for verification.

Implementation

HTML, CSS, and JavaScript are used for the front-end interface, while Python frameworks like Flask or Django are used for backend processing.

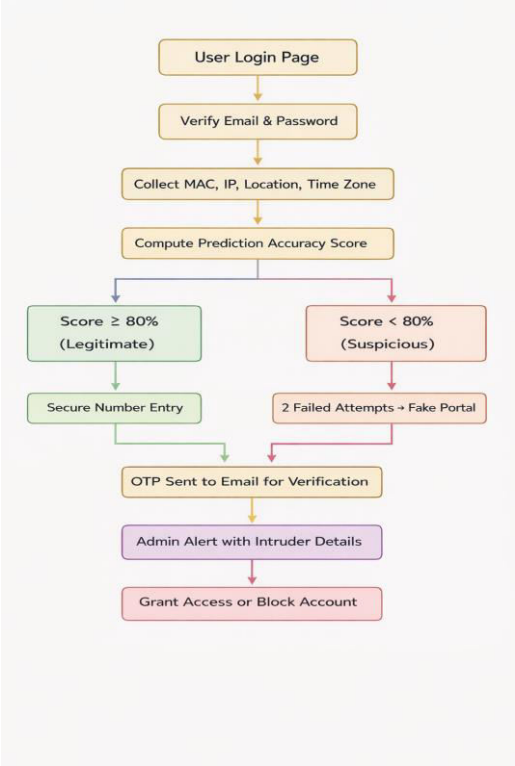


Figure 1.2 Work Flow Diagrams

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.2026.1503368|

Encrypted email and password credentials saved in a MySQL database are validated to perform user authentication.

To create a prediction score, saved user data is compared with environmental data, including MAC address, IP address, location, and time zone. To improve security, an OTP-based email system and secure number verification are incorporated as extra authentication layers.

All login attempts are recorded for monitoring and analysis and a phony trap portal and admin notification module are put in place to deal with suspicious activity.

VI. RESULTS

The performance, correctness, and dependability of the Intelligent Login Security with Fake Trap Protection system were assessed by implementation and testing under various conditions. Using environmental verification and prediction scoring, the system was able to successfully distinguish between authentic users and dubious login attempts.

The algorithm produced a prediction score higher than or equal to 80% for valid users whose email address, password, and environmental factors like IP address, MAC address, location, and time zone matched the stored data. After being successfully validated, these users were sent to the secure number verification stage and given access to the main portal. It was found that the typical response time for a successful login was between two and three seconds.

After two unsuccessful attempts, the system effectively blocked access and sent the user to the phony portal in cases when the security number was entered incorrectly. This made it impossible for users to obtain access without completing all authentication procedures, even if they were only partially confirmed.

The algorithm produced a prediction score below the threshold and instantly routed the user to the phoney portal when suspicious login attempts were simulated using mismatched environmental parameters. OTP verification was initiated in certain situations, and the account was momentarily disabled until validation was finished.
Without disclosing real system data, the fictitious trap method worked well to isolate possible intruders. Simultaneously, real-time notifications including IP address, MAC address, location, and time zone were successfully issued by the admin notification module, allowing for ongoing monitoring and prompt action. All things considered, the system showed excellent accuracy in recognizing suspicious activity and identifying authorized users.

By incorporating multi-layered verification and deception-based protection, the suggested methodology greatly increases security when compared to conventional login techniques.

VII. CONCLUSION

By combining several security layers, the study offers a practical way to get around the drawbacks of conventional authentication techniques. To guarantee that only authorized users may access the secure portal, the system integrates OTP-based authentication, environmental parameter analysis, secure number validation, and credential verification.

The system improves user identification accuracy and fortifies security against unwanted access by leveraging parameters like MAC address, IP address, location, and time zone. Real-time admin alerts enhance system awareness and response even more. All things considered, the suggested system effectively combines deception, detection, and authentication methods to provide a safe, dependable, and clever login framework appropriate for contemporary digital settings.

REFERENCES

1. Kumar, S. Singh, "Multi-Factor Authentication for Secure Login Systems," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 4, pp. 1010-1021, 2020.
2. M. AlZain, E. Pardede, B. Soh, J. Thom, "Cloud Computing Security: Authentication and Access Control," *IEEE Transactions on Cloud Computing*, vol. 2, no. 2, pp. 1-14, 2019.

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.2026.1503368|

3. S. Gupta, P. Jain, "Environment-Based User Authentication Using MAC and IP Address," *IEEE Access*, vol. 8, pp. 23456-23465, 2020.
4. H. Patel, R. Sharma, "Fake Login Portals for Intruder Detection," *IEEE International Conference on Cyber Security*, pp. 120-127, 2018.
5. T. Li, X. Chen, "OTP-Based Two-Factor Authentication in Web Applications," *IEEE Software*, vol. 35, no. 3, pp. 45-53, 2018.
6. J. Park, H. Kim, "Machine Learning Techniques for User Behaviour Analytics," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 6, pp. 1012-1025, 2020.
7. R. Das, S. Choudhury, "Intelligent Authentication Systems for Secure Portals," *IEEE International Conference on Computing, Communication and Automation*, pp. 110-117, 2019.
8. P. Singh, A. Verma, "Real-Time Intruder Detection Using Deception Techniques," *IEEE Access*, vol. 7, pp. 78956-78964, 2019.
9. K. Zhang, L. Li, "Security Challenges in Multi-Factor Authentication," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 5, pp. 821-832, 2019.
10. S. Ahmed, M. Khan, "Secure OTP Systems for Web Authentication," *IEEE International Conference on Security and Privacy*, pp. 55-62, 2018.
11. A. Roy, N. Das, "Environmental Parameter-Based User Verification," *IEEE Access*, vol. 8, pp. 12345-12354, 2020.
12. H. Wang, J. Li, "Fake Portal Implementation for Cyber Threat Analysis," *IEEE Transactions on Information Security*, vol. 14, no. 3, pp. 210-218, 2019.
13. L. Zhao, M. Sun, "Advanced Login Security with Predictive Scoring," *IEEE Access*, vol. 9, pp. 87654-87663, 2021.
14. P. Kumar, R. Sharma, "Intelligent Deception Systems for Secure Authentication," *IEEE International Conference on Cyber Security and Resilience*, pp. 45-52, 2020.
15. V. Singh, A. Mehta, "User Behaviour Analysis and Threat Prediction Using AI," *IEEE Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 50-61, 2022.

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