ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

A Web Security Framework Integrating OTP- Based Multi-Factor Authentication and Cyber Awareness

Ruhee[1]; Prakash O. S.[2]; Dr. Girish Kumar D.[3]

[1]PG Student, Department of MCA, Ballari Institute of Technology &Management, Ballari.
[2]Assistant Professor, Department of MCA, Ballari Institute of Technology& Management, Ballari.
[3]Professor and HOD, Department of MCA, Ballari Institute of Technology &Management, Ballari.

Publication Date: 2026/05/21

Abstract: Web applications increasingly handle sensitive personal and organisational information, so security of user authentication essential. Nowadays traditional password methods sare still common, but they are vulnerable to threats like password reuse, brute force attacks, & phishing. Multi-factor authentication (MFA) offers better access control. Thus however, many systems overlook the human factor, which plays significant role in security incidents. This paper describes the design and implementation of a one time based multi-factor authentication system that includes a cyber awareness chatbot, voice assistant and spam checker. The proposed system improves authentication by combining password validation with email-based one-time password (OTP). It also educates users about common cybersecurity risks through an interactive chatbot. Using the Flask web framework and a MySQL database, the system's experimental evaluation shows stronger resistance to unauthorised access and increased user awareness. This suggests that merging authentication with education can create the more effective security for web applications.

Keywords: *Multi-Factor Authentication, One-Time Password, a Cyber Awareness, Chatbot, Web Application Security, Human Factor Security.*

How to Cite: Ruhee; Prakash O. S.; Dr. Girish Kumar D. (2026) A Web Security Framework Integrating OTP- Based Multi-Factor Authentication and Cyber Awareness. *International Journal of Innovative Science and Research Technology*, 11(5), 885-890. https://doi.org/10.38124/ijisrt/26may311

I. INTRODUCTION

The rapid growth of web-based services has greatly increased the need for secure authentication methods. User authentication is the main entry point to system resources and ensures that access goes only to authorized people. Despite ongoing advancements in cybersecurity, many applications still depends of the solely on password-based authentication. These systems are very vulnerable to breaches caused by weak passwords, password reuse across platforms,and the social engineering attacks that takes place advantage of human trust and mistakes.

Multi-factor authentication has emerged as a solid solution to improve access control by requiring more than one method of verification. Among various MFA techniques, OTP-based authentication is popular due to its low cost and easy deployment. While MFA boosts technical security, it does not completely tackle risks linked to user behavior. Even with strong authentication in place, users may still fall for phishing emails, fake websites, or misleading messages that lead to credential theft.

To address these issues, this research suggests a security framework that combines the factor of OTP-based multi- factor authentication with a cyber awareness chatbot. The chatbot serves as an interactive educational tool that offersreal-time security advice and answers questions about common cyber threats. By providing timely tips and guidance, the chatbot helps users spot and avoid potential attacks while interacting with the system.

In addition to a particular of enhancing user awareness, the proposed framework improves overall usability by offering clear and the simple guidance during user interaction. The integrated chatbot provides security related information within the application, reducing the need for users to depend on external resources. By delivering timely advice and explanations, the system supports better user decision making and promotes safe online behavior.

By combining secure authentication mechanisms with continuous user guidance, the system establishes a well balanced security approach. Addressing both technical security challenges and human related vulnerabilities, the proposed solution delivers a more reliable and user oriented

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

web security model. This makes the system practical and effective for deployment in real world web applications.

II. RELATED WORK

Research in the area of the web applications to security has consistently emphasized the importance of the strong user authentication mechanisms. Password based authentication alone is no longer sufficient due to common issues such as weak password selection, reuse across platforms, and exposure through social engineering attacks. To overcome these limitations, multi factor authentication can be widely adopted. OTP based verification adds an additional security layer by validating user identity dynamically, which significantly reduces the chances of unauthorized access. Email based OTP delivery continues to be widely used because it is simple to deploy and does not require specialized hardware or complex infrastructure.

Alongside authentication research, cybersecurity studies have increasingly highlighted the impact of user behavior on system security. A large number of security incidents occur not because of system flaws, but due to human errors such as clicking malicious links, responding to phishing messages, or sharing sensitive information unknowingly. To mitigate these risks, awareness programs and digital safety training initiatives have been introduced. However, these solutions are often disconnected from the actual authentication process and fail to provide assistance at the moment when users are most vulnerable to attacks.

In recent years, conversational systems such as chatbots have gained attention as effective tools for delivering guidance and support. Their interactive nature allows users to receive instant responses and personalized assistance. In cybersecurity applications, chatbots have been explored as a means to explain threats, provide safety tips, and answer user questions in real time. Despite this potential, most existing implementations treat chatbots as standalone tools rather than integrating them directly into security critical workflows such as authentication.

Many existing authentication systems focus primarily on strengthening access control while overlooking usability and user support. Complex login procedures can confuse users and create frustration, which may lead them to adopt unsafe practices like reusing passwords or attempting to bypass security measures. Research suggests that systems which combine security enforcement with clear guidance and user friendly interaction achieve better acceptance and long term effectiveness.

Recent studies also indicate that security systems benefit from actively engaging users during sensitive operations. Providing real time explanations, warnings, or advice during authentication helps users understand security actions and recognize potential threats. When users are informed and involved, they are more likely to follow safe practices and respond appropriately to suspicious situations.

In summary, integrating strong authentication techniques with interactive user guidance represents a practical direction for improving web security. By addressing both system level protection and human related vulnerabilities in a unified framework, such solutions offer improved security, better usability, and greater suitability for real world web applications.

Furthermore, modern web applications increasingly demand security solutions that can evolve with changing threat landscapes. Static security mechanisms often fail to respond effectively to new attack techniques. Systems that allow flexible updates, modular enhancements, and user centered guidance are better suited for long term deployment. By designing authentication and awareness components as modular units, security frameworks can be improved over time without disrupting existing functionality.

III. PROPOSED FRAMEWORK

- *System Overview*

The proposed framework aims to improve web application security by combining OTP-based system with multi-factor authentication with a cyber awareness chatbot. The system verifies user identity through a two-step process. First, it checks the password, then it verifies a one-time password. In addition to authentication, a chatbot provides real-time cybersecurity advice to users. This combined approach boosts technical security and addresses the human factor, which often contributes to security breaches.

The framework works as a web-based application, allowing users to interact through a browser. The backend processes authentication requests, manages OTP generation and verification, and handles interactions with the chatbot. All user-related data, including credentials, OTP records, login attempts, and chatbot interactions, is securely stored in a centralized database.

- *Key Functional Modules*

The system consists of multiple functional modules that collectively ensure secure access and improved user awareness. The authentication module verifies user credentials by checking the entered username and password. After successful validation, the multi factor authentication process is initiated by generating a one time password. The OTP verification module generates a time limited OTP and delivers it to the user's registered email address. Access is granted only when the correct and valid OTP is submitted, thereby strengthening the login process.

In addition to authentication, the cyber awareness chatbot module plays an important role in user education. It responds to user queries using predefined security focused responses and provides guidance on safe online behavior during system usage. The database management module supports all other components by securely storing and retrieving user data, OTP records, login attempts, and chatbot interactions. The user interface module enables smooth interaction through web pages for login, OTP

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

verification, chatbot communication, and administrative access.

The framework follows a modular architecture in which each component operates independently while remaining connected to the overall system. This design improves maintainability and allows easy scalability for future enhancements. Additional security features or awareness tools can be integrated without affecting existing functionality. By clearly separating authentication, awareness, data handling, and interface responsibilities, the system achieves efficient performance, reliable operation, and a balanced focus on security and usability.

➢ *Visual Overview*

The visual representation of the proposed framework illustrates the interaction between the user, authentication components, chatbot module, and the centralized database. The process begins when a user initiates a login request through the web interface. This request is forwarded to the authentication module, which validates the user credentials and performs OTP verification by communicating with the database. Simultaneously, the chatbot module remains available to interact with the user and provide cybersecurity awareness, offering guidance and clarifying security related concerns during the authentication process. This interaction highlights the seamless integration of secure access control and user education within a single system.

The diagram also demonstrates how all system components are interconnected through a structured flow. Each module communicates efficiently while maintaining a clear separation of responsibilities, ensuring reliable operation and secure data handling. By visually representing these interactions, the architecture emphasizes the balance between strong authentication mechanisms and continuous user support, reinforcing the framework's goal of improving both security and usability in modern web applications.

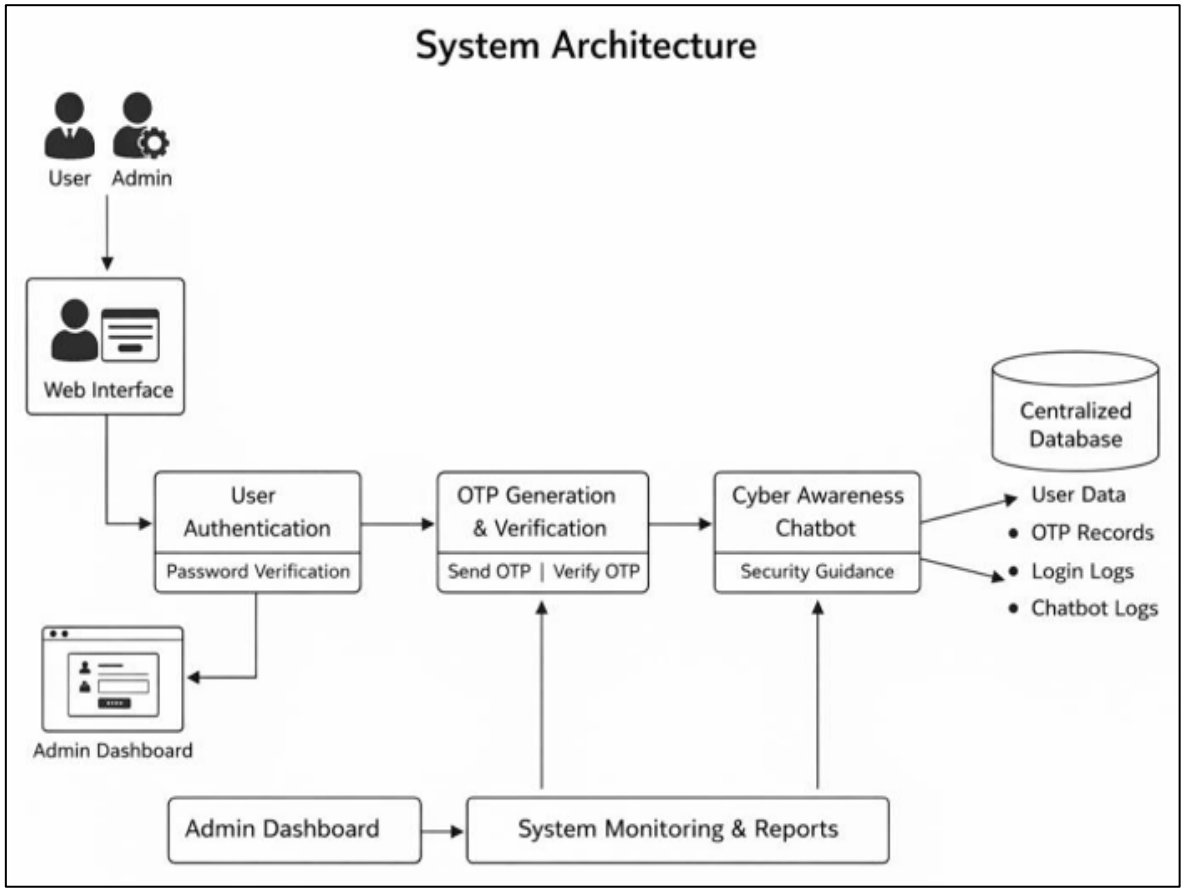

Fig 1 System Overflow

IV. METHODOLOGY AND IMPLEMENTATION

➢ *Methodology*

The proposed system follows a structured methodology that integrates secure authentication mechanisms with user awareness support to address both technical vulnerabilities and human related security risks. The workflow begins when a user accesses the web application and submits login credentials through the user interface. These credentials are forwarded to the authentication module, where they are validated against securely stored user information in the database.

Once the initial credential verification is successful, the system initiates the second layer of authentication as part of the multi factor authentication process. A one time password is dynamically generated and sent to the user's registered email address. The OTP is designed with a short validity period to minimize the risk of unauthorized use. The user must submit the received OTP within the allowed

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

time frame, after which the system verifies both its correctness and expiration status. Access is granted only when all verification conditions are satisfied, ensuring enhanced protection even if primary credentials are compromised.

Throughout this process, the cyber awareness chatbot operates alongside authentication functions. The chatbot provides predefined responses related to common cybersecurity threats such as phishing, malware, and unsafe password practices. By offering real time guidance during user interaction, the system encourages informed decision making and reduces the likelihood of security incidents caused by user error. This combined approach ensures a balanced focus on access control and user awareness.

- *Implementation*

The framework is implemented as a web based application using the Flask framework, chosen for its simplicity, flexibility, and support for modular development. Flask acts as the central controller, handling user requests, routing, session management, and communication between different modules. The authentication logic, OTP generation and verification, chatbot responses, and admin functionalities are implemented as separate components to improve maintainability.

A MySQL database is used as the backend data storage system. It securely stores user credentials, OTP records, login attempts, and chatbot interaction logs. Passwords are stored in encrypted form to prevent exposure of sensitive information. OTP details are logged with timestamps to support validation and auditing. The chatbot module uses predefined response sets to provide consistent and reliable cybersecurity guidance.

The user interface is developed using standard web technologies, allowing users and administrators to interact with the system through a browser. This implementation ensures smooth integration between security enforcement, awareness delivery, and system monitoring. The modular design also allows future enhancements, such as adding new authentication factors or expanding chatbot capabilities, without affecting the core system functionality.

V. RESULTS AND DISCUSSIONS

The proposed security framework was evaluated under different usage conditions to measure its effectiveness, stability, and user experience. Test cases included valid login attempts, incorrect passwords, expired OTP entries, and wrong OTP inputs. In all scenarios, the system strictly followed the multi-factor authentication process. Access was granted only when both the password and the one-time password were verified successfully. This confirms that the framework is capable of preventing unauthorized access even if one authentication factor is compromised.

The OTP mechanism performed reliably during testing. One-time passwords were generated dynamically for each session and delivered to the registered email address within an acceptable time frame. OTPs were valid only for a short duration, and expired codes were automatically rejected. This behavior minimizes the risk of replay attacks and enhances overall access control. All OTP-related activities, including generation, validation, and failure cases, were accurately recorded in the database, supporting effective monitoring and future analysis.

System performance was analyzed by observing response time and consistency during repeated authentication requests. The backend processed password verification and OTP validation efficiently without noticeable delays. Even during multiple consecutive login attempts, the application remained stable. The lightweight framework and optimized database operations contributed to smooth execution, indicating that the system is suitable for real-world deployment.

The cyber awareness chatbot significantly enhanced user interaction and security understanding. During evaluation, the chatbot responded clearly to user queries related to phishing threats, malware risks, and secure password practices. By offering guidance directly within the system, users were able to obtain security information instantly without relying on external sources. This immediate support helped reduce confusion and promoted safer user behavior during authentication.

From a usability perspective, the integration of security features did not complicate the login process. The user interface provided clear instructions and feedback at each stage of authentication. The chatbot further supported users by explaining security prompts and best practices in simple terms. This balance between strong security enforcement and ease of use is one of the key strengths of the proposed framework.

Another important outcome of the evaluation was the effectiveness of activity logging. Records of login attempts, OTP usage, and verification results offered valuable insight into system usage patterns. These logs enable administrators to identify suspicious behavior such as repeated failures or abnormal access attempts, allowing timely responses to potential threats. Additionally, this data can support future system enhancements and policy improvements.

Overall, the results demonstrate that integrating OTP-based multi-factor authentication with a cyber awareness chatbot provides better protection than traditional password-only systems. By addressing both technical security requirements and human-related risks, the proposed framework delivers a more secure, reliable, and user-friendly solution for modern web applications.

VI. CONCLUSION

This work presents a secure web authentication framework that combines OTP-based multi-factor authentication with a cyber awareness chatbot. The proposed system strengthens traditional login methods by adding another verification step, which helps reduce the risk

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

of unauthorized access. By enforcing time-limited OTP validation, the framework addresses common weaknesses found in password-only authentication systems.

Along with technical security, adding a cyber awareness chatbot adds real value by tackling human-related security risks. That the chatbot gives offers to real-time guidance on cybersecurity threats and safe practices while users interact with the system. This approach improves user understanding and promotes responsible behavior, which is key in preventing security breaches caused by human error.Overall, this results in a show that has the combining authentication and awareness in one framework leads to a more secure and user-friendly system. The modular design, efficient performance, and better user engagement suggest that the proposed solution is practical for real-world web applications. This work emphasizes the importance of merging security measures with user education to develop effective and lasting cybersecurity solutions.

FUTURE WORK

The proposed security framework can be further strengthened by incorporating additional authentication factors to enhance identity verification. Biometric techniques such as fingerprint scanning or facial recognition can be integrated to provide stronger assurance of user identity. Exploring alternative OTP delivery mechanisms, including mobile authenticator applications, push notifications, or SMS-based verification, may improve reliability and user convenience, especially in environments with limited email access.

The cyber awareness chatbot also offers considerable scope for enhancement. Future versions of the chatbot can be designed with adaptive behavior, allowing it to refine responses based on user interaction patterns. Personalized security suggestions and situation-based guidance could increase user engagement and learning effectiveness. Expanding language support would further improve accessibility and ensure the system can serve users from different regions and backgrounds more effectively.

Another area for future development involves improving system monitoring and analysis capabilities. Advanced logging mechanisms combined with behavior analysis can help detect suspicious patterns such as repeated failed login attempts or unusual access times. Incorporating anomaly detection techniques would enable early identification of potential threats, allowing administrators to respond proactively.

In addition, integrating machine learning techniques could improve the accuracy of threat detection and user behavior analysis. By learning from historical login data and interaction logs, the system could identify subtle security risks that traditional rule-based approaches might miss. This would further strengthen the system's ability to adapt to evolving cyber threats.

Finally, large-scale testing under real-world conditions is an important direction for future work. Evaluating system performance with a higher number of users and simultaneous login attempts would provide insights into scalability and robustness. Such evaluations would help optimize performance and ensure long-term reliability, making the framework suitable for deployment in enterprise-level environments.An additional improvement to the system is introducing permission-based access management. By defining specific privileges for different types of users, the application can control which features and data each user can access. This is especially helpful in organizational settings where system administrators, employees, and general users have different roles. Limiting access to only what is necessary helps reduce security risks and the potential impact of unauthorized actions.

The system can also benefit from easier maintenance and long-term deployment support. Automating software updates and security fixes would help protect the application from new threats. Moving the framework to a cloud environment could further improve system availability, support higher traffic, and boost reliability. These changes would ensure smoother operation and help the system respond better to future security and technology needs.

REFERENCES

[1]. L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
[2]. A. Herzberg, "Payments and banking with mobile personal devices," *Communications of the ACM*, vol. 46, no. 5, pp. 53–58, 2003.
[3]. S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security*, 3rd ed., O'Reilly Media, 2003.
[4]. F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641–644, 2009.
[5]. P. Inglesant and M. A. Sasse, "The true cost of unusable password policies," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 383–392, 2010.
[6]. M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password Cracking Using Probabilistic Context-Free Grammars," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 391–405, 2010.
[7]. N. Gruschka, L. Lo Iacono, and N. Luttenberger, "Security Issues in Web-Based Applications," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 22–29, 2014.
[8]. K. Fawaz and K. G. Shin, "Location privacy protection for smartphone users," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 239–250, 2014.
[9]. A. B. Johnston and S. Weidner, "Usability and Security: Evaluating Authentication Systems," *IEEE Computer*, vol. 48, no. 12, pp. 54–61, 2015.
[10]. J. Lester and J. Branting, "Interactive Chatbots for

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may311

User Assistance and Learning," *Artificial Intelligence Review*, vol. 34, no. 1, pp. 1–16, 2016.

[11]. M. Conti, N. Dragoni, and V. Lesyk, "A survey of man- in-the-middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[12]. R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with machine learning," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 40–47, 2016.

[13]. S. Furnell and K. Evangelatos, "Public Awareness and User Education in Information Security," *Computer Fraud & Security*, no. 6, pp. 8–13, 2017.

[14]. K. Renaud and M. Goucher, "The Role of Human Behavior in Cybersecurity," *Journal of Cybersecurity*, vol. 3, no. 1, pp. 1–14, 2017.

[15]. R. B. Basnet and A. H. Sung, "User Authentication and Authorization Frameworks in Modern Web Systems," *Journal of Information Security*, vol. 8, no. 2, pp. 87–98, 2018.

[16]. A. B. Johnston, "Authentication usability and security trade-offs in web applications," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 72–75, 2018.

[17]. T. Jensen, M. Dürmuth, and B. Fabian, "Security awareness and user behavior in authentication systems," *Proceedings of the International Conference on Information Security*, pp. 101–115, 2018.

[18]. A. O. Adewumi, O. Bello, and S. Misra, "Multi-Factor Authentication Techniques for Secure Web Applications," *International Journal of Computer Security*, vol. 12, no. 3, pp. 45–53, 2019.

[19]. M. Alzubaidi, A. Abuhussein, and M. Shurman, "One- Time Password Authentication Systems: A Survey," *International Journal of Network Security*, vol. 21, no. 4, pp. 623–632, 2019.

[20]. OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2023