Scholar J

https://doi.org/10.67378/sj/178

Research Article

Design and Implementation of a Secure Web-Based Messaging Application Using Bcrypt Authentication

Enenche Ngbede Michael[1], Aminu Muhammad Adamu[2] and Collins Ifeanyi Osuji[3]

[1]Department of Cybersecurity, Nigerian Defence Academy, Kaduna, Nigeria.

[2]Department of Compute Science, Nasarawa State University, Keffi, Nigeria.

[3]Department of Computer Science, Federal University, Wukari, Nigeria.

Received 13 May 2026; Acceptance 15 June 2026; Published 21 June 2026.

Abstract

The increasing reliance on digital communication has heightened concerns regarding the security and privacy of sensitive information exchanged through messaging platforms. Conventional communication systems remain vulnerable to unauthorized access, message interception, data breaches, and weak authentication mechanisms, thereby necessitating the development of more secure communication solutions. This study presents the design and implementation of a secure web-based messaging application that integrates user authentication, secure message management, and database security within a unified framework. The system was developed using the V-Model software development methodology and implemented using Laravel, PHP, MySQL, HTML, JavaScript, and JQuery. To enhance credential security, the Bcrypt hashing algorithm was employed for password protection and user authentication. Functional testing was conducted to evaluate key system operations, including user registration, login authentication, message transmission, message retrieval, and database management. The results indicate that the developed application successfully achieved all intended functionalities, providing reliable user authentication, efficient message management, and secure access control. Furthermore, the system demonstrated satisfactory performance in terms of reliability, usability, and data integrity. The study contributes to the development of secure communication systems by integrating authentication and database security mechanisms within a web-based messaging environment. It is concluded that the proposed system provides a practical and scalable framework for confidential communication among authorized users. Future enhancements may incorporate advanced end-to-end encryption protocols and multi-factor authentication to further strengthen system security.

Correspondence addressed to Enenche N. Michael, email:michaelenenche3@gmail.com

Keywords: Secure Messaging Application, Authentication, Bcrypt, Web Security, Access Control, Database Security.

Introduction

The rapid growth of information and communication technologies has revolutionized digital communication, making messaging applications indispensable tools for individuals, organizations, and government institutions. Despite their widespread adoption, these platforms remain vulnerable to security threats such as unauthorized access, eavesdropping, message interception, identity theft, and cyber espionage, which compromise the confidentiality, integrity, and authenticity of sensitive information.

To mitigate these threats, secure messaging systems incorporating cryptographic techniques have gained considerable attention. End-to-end encryption (E2EE) is widely regarded as one of the most effective approaches for protecting digital communications, as it ensures that only the intended sender and recipient can access message contents [1]. Consequently, modern messaging applications such as WhatsApp, Signal, Telegram, and Viber have integrated encryption mechanisms to enhance privacy and communication security.

Several researchers have proposed secure communication solutions using different cryptographic algorithms. Ali and Sagheer in [2] developed a secure Android messaging application based on ECDH, AES, and RC4 algorithms, while Sabah et al. [3] implemented an end-to-end encrypted chat system using AES and RSA. Comparative studies [4-5], further highlighted the importance of robust encryption and authentication mechanisms in modern messaging platforms.

Despite these advances, existing studies largely focus on specific cryptographic algorithms or mobile-based implementations, with limited emphasis on integrating secure authentication, access control, database security, and encrypted communication within a unified web-based framework. Furthermore, many existing solutions provide limited flexibility for organizational environments that require centralized management and controlled access to sensitive information.

The persistence of unauthorized access, weak authentication mechanisms, and message interception underscores the need for a secure messaging platform that combines strong user authentication with secure message management. Therefore, this study presents the design and implementation of a secure messaging application that integrates authentication, secure database management, and cryptographic security techniques to enhance the confidentiality, integrity, and reliability of digital communication.

Materials and Methods

This study adopted a developmental research approach to design and implement a secure web-based messaging application. The system was developed using the V-Model software development methodology, which links each development stage with a corresponding testing phase to improve software reliability and quality assurance [6-7].

The proposed system comprises four major modules: User Management, Messaging, Encryption, and Database Management. User authentication and password security were implemented using the Bcrypt hashing algorithm, while the application was developed using the Laravel MVC framework with PHP, HTML, JavaScript, and JQuery. MySQL was employed for data storage and management, with the database consisting of Users, Messages, and Message Replies tables interconnected through a relational structure [8-10].

System testing focused on validating core functionalities, including user registration, login authentication, message transmission, message retrieval, and database operations. The system architecture was designed to ensure confidentiality, reliability, scalability, and secure communication among authorized users.

Results and Discussion

System Architecture

The developed secure messaging application adopts a three-tier architecture consisting of the presentation, application, and database layers. The presentation layer provides the user interface through which users interact with the system, while the application layer processes user requests, authentication, and message management. The database layer stores user information, messages, and message replies. This architecture enhances modularity, scalability, and maintainability of the system.

The integration of authentication, message management, and database services within a unified framework enables secure communication among authorized users while ensuring efficient data storage and retrieval.

Authentication Mechanism

User authentication was implemented using the Bcrypt hashing algorithm to protect user credentials from unauthorized access. During registration, user passwords are hashed before storage in the database. During login, the entered password is verified against the stored hash, ensuring that plaintext passwords are never stored or transmitted.

Table 1. Authentication Features Implemented.

Feature	Description	Status
User Registration	Creation of user account	Implemented
Password Hashing	Bcrypt encryption of passwords	Implemented
User Login	Credential verification	Implemented
Session Management	Authorized access control	Implemented

Feature	Description	Status
Password Reset Support	Recovery mechanism	Implemented

The use of Bcrypt strengthens password security by incorporating salting and adaptive hashing mechanisms, thereby reducing vulnerability to brute-force and rainbow-table attacks.

Database Design

The database was designed using a relational structure comprising three principal tables: Users, Messages, and Message Replies. Relationships among these tables facilitate efficient communication tracking and message management.

Table 2. Core Database Tables.

Table	Purpose
Users	Stores user profile and authentication information
Messages	Stores transmitted messages between users
Message Replies	Stores responses associated with messages

The relational design improves data integrity by maintaining logical connections between users and communication records while minimizing data redundancy.

System Testing and Performance Evaluation

Functional testing was conducted to verify the performance of major system components. The tests focused on user authentication, message transmission, message retrieval, and database operations.

Table 3. Functional Testing Results.

Test Case	Expected Result	Actual Result	Status
User Registration	User account created successfully	Successful	Pass
User Login	Authorized access granted	Successful	Pass
Message Sending	Message stored and delivered	Successful	Pass
Message Retrieval	Messages displayed correctly	Successful	Pass
Reply Function	Reply linked to original message	Successful	Pass

Test Case	Expected Result	Actual Result	Status
Database Update	Records updated correctly	Successful	Pass

The testing results indicate that all major functionalities operated according to system specifications. No significant errors were observed during system validation, demonstrating the reliability of the developed application.

Table 4. System Performance Evaluation.

Performance Metric	Observation
Response Time	Fast and acceptable for real-time communication
Data Integrity	Maintained throughout testing
Reliability	Stable system operation observed
Scalability	Supports future expansion of users and messages
Usability	Simple and user-friendly interface

The system exhibited satisfactory performance under normal operating conditions, supporting efficient message exchange and data management.

Security Analysis

Security evaluation focused on the effectiveness of authentication and data protection mechanisms implemented within the system.

Table 5. Security Features and Benefits.

Security Feature	Security Benefit
Bcrypt Password Hashing	Protects stored user credentials
Authentication Control	Restricts access to authorized users
Session Validation	Prevents unauthorized system usage
Relational Database Structure	Preserves data consistency and integrity
Access Control Mechanism	Enhances confidentiality of communication

The implementation of Bcrypt significantly improves password security by generating computationally expensive hashes that are resistant to brute-force attacks. Furthermore, authentication and access-control mechanisms ensure that only authorized users can access communication resources. The database design also contributes to system security by maintaining the integrity and traceability of communication records.

Overall, the developed secure messaging application successfully achieved its primary objectives of providing secure user authentication, efficient message management, and reliable communication services. The results demonstrate the feasibility of integrating authentication and database security mechanisms into a unified messaging platform for confidential communication.

Discussion of Findings

Authentication Mechanism

Table 1 presents the authentication features implemented in the developed system. The results show that user registration, login verification, password hashing, session management, and password recovery functionalities were successfully integrated into the application. The use of the Bcrypt hashing algorithm ensures that user passwords are stored in an encrypted format rather than as plaintext, thereby enhancing resistance to brute-force and rainbow-table attacks [10].

These findings are consistent with the work of [4], who emphasized the importance of integrating authentication mechanisms with cryptographic security to improve the confidentiality of communication systems. Similarly, weak authentication mechanisms were identified as a major vulnerability in messaging platforms and recommended stronger access control measures [5]. Unlike many existing messaging applications that focus primarily on message encryption, the developed system incorporates authentication as a core security component, thereby providing an additional layer of protection against unauthorized access.

Database Design

Table 2 summarizes the core database structure of the developed application. The Users, Messages, and Message Replies tables provide a relational framework for managing user information and communication records. The relational design facilitates efficient storage, retrieval, and management of messages while preserving data integrity.

The database architecture aligns with the recommendations of [4], who noted that secure messaging systems require not only encryption mechanisms but also reliable data management structures to ensure the integrity of communication records. Furthermore, the use of linked database entities improves traceability and accountability within the system, which is particularly important in organizational environments where communication records may require monitoring and auditing.

Compared with the mobile-centric architectures proposed by [2-3], the present system adopts a web-based relational framework that provides centralized management of users and communication data, thereby enhancing scalability and administrative control.

System Testing and Performance Evaluation

The functional testing results presented in Table 3 indicate that all major system operations performed successfully. User registration, authentication, message transmission, message retrieval, and reply functionalities achieved the expected outcomes without operational errors. These results demonstrate that

the developed system satisfies its functional requirements and is capable of supporting secure communication among authorized users.

The performance evaluation results shown in Table 4 further reveal that the application exhibits acceptable response times, reliable operation, and effective data management capabilities. The observed reliability suggests that the system architecture and database design are adequate for supporting routine communication activities.

These findings corroborate those of [3], who reported successful implementation of a secure messaging platform using cryptographic techniques to protect communication data. Similarly, [2] demonstrated that the integration of security mechanisms within messaging applications can improve communication reliability and confidentiality. However, unlike these studies, which focused primarily on cryptographic message protection, the present study additionally incorporates user authentication, session management, and database security within a unified framework.

Security Analysis

Table 5 presents the major security features implemented in the system and their associated benefits. The results indicate that Bcrypt-based password hashing, authentication control, session validation, and access control mechanisms collectively contribute to the security of the platform. These features help ensure that only authorized users can access communication resources while protecting stored credentials from unauthorized disclosure.

The findings support the observations of [1], who argued that secure communication systems require multiple layers of protection beyond message encryption alone. While previous studies by [2,3,4] primarily concentrated on cryptographic protection of transmitted messages, the present study demonstrates the importance of integrating authentication and database security mechanisms into the overall communication framework.

Moreover, the implemented security architecture addresses some of the limitations identified by [4-5], particularly regarding user authentication and access control. Although the system currently relies on Bcrypt for credential protection rather than full end-to-end message encryption, the results indicate that it provides a secure foundation for confidential communication and can be extended in future work through the integration of advanced encryption protocols such as AES, RSA, or the Signal Protocol.

Overall, the results demonstrate that the developed secure messaging application successfully integrates authentication, database security, and communication management within a single platform. The system addresses several shortcomings identified in previous studies and provides a practical framework for secure organizational communication.

Conclusion

This study presented the design and implementation of a secure web-based messaging application aimed at enhancing the confidentiality and security of digital communication. The system was developed using

the V-Model software development methodology and integrated user authentication, secure message management, and relational database technologies within a unified framework. Password security was strengthened through the implementation of the Bcrypt hashing algorithm, ensuring secure storage and verification of user credentials. The results demonstrated that the developed application successfully achieved its core functionalities, including user registration, authentication, message transmission, message retrieval, and database management. Functional testing confirmed the reliability and effectiveness of the system, while the security analysis showed that the implemented authentication and access-control mechanisms provide protection against unauthorized access and credential compromise.

Compared with existing studies that primarily focus on message encryption techniques, the developed system emphasizes the integration of authentication, access control, and secure data management within a web-based communication environment. This approach addresses some of the limitations identified in previous secure messaging solutions, particularly in relation to centralized user management and organizational communication requirements. Overall, the study demonstrates the feasibility of developing a secure messaging platform capable of supporting confidential communication among authorized users. Future work should focus on incorporating advanced end-to-end encryption mechanisms such as AES, RSA, or the Signal Protocol, as well as multi-factor authentication and cloud-based deployment, to further enhance the security and scalability of the system.

References

1. Marlinspike, M. & Perrin, T. (2016). "The Double Ratchet Algorithm." Retrieved from Signal Blog.
2. Ali, A., & Sagheer, A. (2017). Design of secure chatting application with end to end encryption for android platform. *Iraqi Journal for Computers and Informatics*, *43*(1), 22-27.
3. Sabah, N., Kadhim, J. M., & Dhannoon, B. N. (2017). Developing an end-to-end secure chat application. *Int. J. Comput. Sci. Netw. Secur*, *17*(11), 108-113.
4. Botha, J., Vant, W. C., & Leenen, L. (2019). A comparison of chat applications in terms of security and privacy. In *Proc. 18th Eur. Conf. Cyber Warfare Secur* (p. 55).
5. Kadhim, M. F., Al-Janabi, A., Alhilali, A. H., & Ali, N. S. (2022). Security approach for instant messaging applications: viber as a case study. *Indonesian Journal of Electrical Engineering and Computer Science*, *26*(2), 1109-1115.
6. Davies, G. T., Faller, S., Gellert, K., Handirk, T., Hesse, J., Horváth, M., & Jager, T. (2023, August). Security analysis of the whatsapp end-to-end encrypted backup protocol. In *Annual International Cryptology Conference* (pp. 330-361).
7. Tariq,U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review, Sensors, vol. 23, no. 8, p. 4117. https://doi.org/10.3390/s23084117.

8. Saharan, M., Kumar, N., Kumar, V., & Juneja, A. (2024). Secure End-to-End Chat Application: A Comprehensive Guide. *Review of Computer Engineering Studies*, *11*(3).
9. Parkar, V. V., Shinde, P. P., Gadade, S. C., & Shinde, P. M. (2016). Utilization of Laravel framework for development of web based recruitment tool. *Iosr Journal of Computer Engineering (Iosr-Jce)*, 36-41.
10. Dan Arias. (2021). HASHING - Hashing in Action: Understanding bcrypt. *Retrieved from: https://auth0.com/blog/hashing-in-action-understanding-bcrypt/*