A MULTI-LEVEL ENCRYPTION TECHNIQUES USING BLOWFISH AND ADVANCED ENCRYPTION STANDARD (AES) TO SECURE JOB PORTAL

BY

Gbolagade Morufat Damola, **Bello Abdulmujeeb**, **Abdulwahab Muhammed Damilare** & **Abubakar Abeeb Olamilekan**

Department of Computer Science, Al-Hikmah University Ilorin, Nigeria
Email: dammyconsult@gmail.com, babdulmujeeb@gmail.com, dashandashan78@gmail.com, olalekz001@gmail.com

Abstract

This study developed a multi-level encryption framework that integrates Blowfish and Advanced Encryption Standard (AES) algorithms with Role-Based Access Control (RBAC) in a PHP-based job portal. The methodology involved the design and implementation of a secure web application using PHP, MySQL, and OpenSSL libraries. Blowfish (via bcrypt) was applied for password hashing, AES-256 for sensitive data encryption, and RBAC for access differentiation between users and administrators. System performance was evaluated using metrics such as encryption/decryption time, throughput, and input validation. Experimental results showed that Blowfish provided strong password protection, while AES-256 achieved efficient encryption of large files such as uploaded CVs. The measured encryption time ranged from 0.016 s to 0.043 s, and decryption time from 0.026 s to 0.086 s, with throughput values between 820.04 KB/s and 1625.74 KB/s, indicating high processing efficiency for small- to medium-sized data. The performance analysis further revealed that throughput generally improved with file size up to a threshold, after which minor fluctuations occurred due to computational overhead.
Keywords: Job Portal, Encryption, Blowfish, Encryption Techniques

Introduction

A job portal, also known as a career portal or job listing websites, is a modern name for an online job board that helps applicants find jobs and aids employers in their quest to locate ideal candidates (Padwal, 2023). Online job listing systems or job portals have grown in popularity as a more accessible and cost-effective alternative to traditional recruitment methods (Arman, 2023). The Online job portal system serves as a tool that links companies with job seekers (Arunthathi *et al*., 2024). These platforms serve as intermediaries, allowing job seekers to view vacancies and employers to post job openings in real time posing as critical digital platforms facilitating employment opportunities by linking employers and job seekers in a dynamic and efficient manner (Nguyen & Wu, 2019). With the proliferation of internet-based recruitment, job portals have become indispensable tools in the labor market ecosystem (Ahmed *et al*., 2020). Despite their popularity, these platforms face several critical challenges, particularly in the areas of security. Many job portals are susceptible to unauthorized access, data breaches, and inefficient access control mechanisms, making them vulnerable to malicious attacks (Kumar & Sharma, 2021). However, the sensitive nature of user data involved including personal information, CVs, and organizational details has made these platforms targets for cyberattacks (Kumar & Mallick, 2018). Data breaches and identity theft are now major concerns, especially in developing countries where cybersecurity infrastructures are still maturing (Okediran & Omole, 2020). Despite the immense benefits of online job portals, several challenges including fake job listings, spam accounts, and data privacy issues are co mmonly reported (Sathiya & Mohanapriya, 2025).

According to Robert *et al.* (2024), cryptographic techniques are strong security measures which are critical to protecting data, maintaining system integrity and fostering trust in applications because they offer diverse tools to address these challenges (Daoui *et al*, 2023; Ahmed *et al*, 2024; Sabrina *et al* 2024). The most widely used cryptographic methods include symmetric cryptography e.g., Blowfish, Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard (AES); asymmetric cryptography e.g., Rivest–Shamir–Adleman (RSA), Digital signature algorithm (DSA), and Elliptic curve cryptography (ECC); hash functions e.g., Secure Hash Algorithm 1 (SHA-1, SHA-2, and SHA-3) (Kaushik *et al*. 2023 Kwatra *et al*., 2024; Selmy *et al*. 2024)(35-38). Cryptography comprises three fundamental components: encryption, decryption, and key. Encryption conceals the original text (plaintext), while decryption reverses the process by converting encrypted text back to plaintext. Both encryption and decryption employ a confidential code, referred to as a key (Zied *et al*., 2023),

Literature Review

The evolution of web technologies has transformed traditional job-seeking practices, making online job portals a major platform for recruitment and employment opportunities. Despite their usefulness, these platforms are susceptible to security breaches due to poor implementation of access control and weak password management practices (Afolabi *et al*., 2021). The increasing reliance on web-based platforms for employment-related services has brought about significant security challenges, particularly in the storage and management of sensitive user data. Job portals serve as critical intermediaries between job seekers and employers, necessitating the implementation of robust security mechanisms to protect personal and corporate information from unauthorized access, data breaches, and cyberattacks. This chapter presents a comprehensive review of existing literature relevant to web application security, cryptographic techniques, and access control models, with particular focus on their application in PHP-based systems. The literature review begins by exploring general job or career or recruitment web applications, its vulnerabilities. It then examines the principles of web security architectures such as cryptography and explores the principles and applications of cryptography, with specific attention to the Blowfish and Advanced Encryption Standard (AES) algorithms. The review further investigates the role of Role-Based Access Control (RBAC) as a logical and structured approach to managing user permissions within multi-role environments like job portals. Previous studies on secure system design, encryption performance, and access control efficiency are analyzed to highlight gaps and justify the relevance of the current study. This chapter aims to provide the theoretical foundation upon which the implementation and security enhancement of a PHP-based job portal can be built. It also identifies best practices, limitations of existing models, and opportunities for improvement using a combined approach of encryption and structured access control.

Methodology

This chapter outlines the methodological framework employed in the development of the proposed web-based job listing application. It describes the research design, tools and technologies, software development approach, system

architecture and evaluation techniques. Figure 1 shows the security architecture.

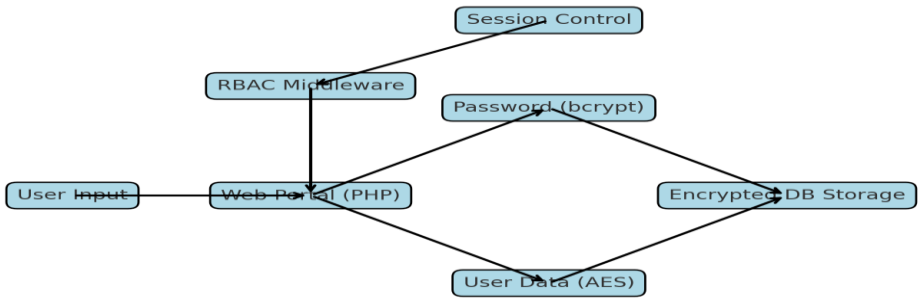

Figure 1: **Security Architecture**

Tools and Technologies to be used for the Development of Job Portal Web Application

The system was built using a technology stack that emphasizes functionality, compatibility, and security:

i. **Backend**: PHP 8.3
ii. **Frontend**: HTML5, CSS3, JavaScript (with Bootstrap)
iii. **Database**: MySQL
iv. **Security Libraries**: PHP's password_hash() and password_verify()
v. **Version Control**: Git and GitHub
vi. **Server Environment**: Apache (XAMPP stack for local testing)
vii. **Testing Tools**: OWASP ZAP, Postman, Laragon

Evaluation and Testing Techniques

The system was evaluated using both **qualitative** and **quantitative** methods:

Functional Testing:

i. Black-box testing of all modules (Registration, Login, Job Posting)
ii. Validation of role access to restricted pages

Cryptographic Testing:

i. Manual and automated brute-force attacks against bcrypt
ii. AES key exposure tests
iii. Input tampering and IV-reuse simulations

Security Testing: OWASP ZAP, Burp suite and SQLMap was used to scan for vulnerabilities (SQL injection, XSS, etc.).

Performance Evaluation

To determine the efficiency of the cryptographic implementation, the system was evaluated using the following key performance metrics**:** Encryption/Decryption Time, Throughput and Input Validation / Injection.

Result

Performance and Evaluation Metrics

To evaluate the effectiveness and efficiency of the implemented cryptographic techniques in the job listing portal, it was necessary to define measurable **performance metrics**. These metrics provide insights into the computational overhead introduced by the encryption and decryption processes, as well as the overall system responsiveness during CV uploads. The selected metrics **encryption time, decryption time, and throughput** are widely used in cryptographic performance analysis (Ahamed & Srinivas, 2021; Sethi & Choubey, 2022).

Encryption Time

Encryption time refers to the duration taken by the algorithm to transform plaintext (the uploaded Credentials) into ciphertext using a secret key. In this research, encryption time was measured in seconds and was captured immediately when a user submitted a CV through the job application form.

Table 4.2: Encryption Time

File Name	File Size (KB)	Encryption Time (s)
A	23.1	0.016431
B	56.6	0.034815
C	30.1	0.026269
D	34.9	0.042559
E	35.1	0.025813

Decryption Time

Decryption time represents the time taken to revert ciphertext back into its original plaintext form using the appropriate decryption key. It was necessary to measure this metric to assess system responsiveness during data retrieval.

Table 4.3: Decryption Time

File Name	File Size (KB)	Decryption Time (s)
A	23.1	0.026448
B	56.6	0.055574
C	30.1	0.035614
D	34.9	0.086400
E	35.1	0.033429

Throughput

Throughput is the rate at which data (in this case, applicant CVs) is processed by the cryptographic algorithms. It reflects the efficiency of encryption and decryption relative to the file size and is expressed in kilobytes per second (KB/s) (Sethi & Choubey, 2022). CV files of varying sizes were used to ensure comprehensive testing.

Table 4.3: Throughput

File Name	File Size (KB)	Encryption Time (s)	Decryption Time (s)	Throughput (KB/s)
A	23.1	0.016431	0.026448	1405.78
B	56.6	0.034815	0.055574	1625.74
C	30.1	0.026269	0.035614	1145.84
D	34.9	0.042559	0.086400	820.04
E	35.1	0.025813	0.033429	1359.78

Conclusion

The developed job portal employs a multi-level encryption strategy to protect user data. In the designed job portal, applicant credentials ranging from (name, email, and other personal details) and CV files which are uploaded are encrypted on submission, and only authorized administrators can decrypt and view them. In particular, the system uses the Blowfish cipher (via the bcrypt hash function) for password storage and the AES-256 block cipher for encrypting CV files. This is inline with the work of Purwinarko & Hardyanto in 2018 where the hybrid Security Algorithm of AES and Blowfish was adopted for Authentication in Mobile Applications. It is could be stated that this layered approach leverages the strengths of both algorithms: Blowfish (with bcrypt) provides a strong salted hash for authentication data, while AES-256 delivers high-speed, high-security encryption of larger documents. Such multi-layer protection is in line with hybrid encryption adopted by computer scientist. The Multi-Level Encryption system developed successfully achieved its goal of securing a job portal by encrypting sensitive user data and credentials with both Blowfish and AES-256 algorithms. By design, user passwords and profile information are first processed with a Blowfish layer and then further encrypted with AES-256 before storage, providing layered protection. This dual-layer approach combines Blowfish's low-overhead speed with AES-256's strong, standardized security, ensuring that data remains unintelligible to unauthorized parties. The implementation integrates Role-Based Access Control (RBAC) to enforce least-privilege policies: only users assigned specific roles may view or manage protected resources, thereby reducing the attack surface. As a result, the core achievement of this work is a prototype job portal where all critical data is encrypted-in-use and encrypted-at-rest, access is tightly controlled, and user interactions remain fully functional and responsive.

Recommendations

i. Future work should explore hybrid cryptosystems that integrate asymmetric algorithms (RSA/ECC) for key exchange, automated key rotation, and the use of secure key management services (KMS/HSM) for enterprise deployment.
ii. Migrating to cloud-native infrastructure using microservices and containerization will ensure elasticity and modular maintenance. Database optimization and caching should be employed to handle high-volume traffic efficiently.
iii. Biometric authentication, when paired with MFA, can further reduce impersonation risks. Comprehensive audit logging should be implemented to satisfy regulatory needs and strengthen accountability.

iv. Partnering with recruitment platforms and industry stakeholders would validate the system under real-world load and security requirements. Academic–industry collaboration could also yield optimizations and encourage adoption of secure architectures in broader e-recruitment contexts.

References

Ahmed AI, Gani A, Ab Hamid SH, Abdelmaboud A, Syed HJ, Mohamed RA, Ali I (2024). Service management for IoT: requirements, taxonomy, recent advances and open research challenges. IEEE Access. 2019 Oct 17, 7:155472-88.

Arman, M. (2023). The Advantages of Online Recruitment and Selection: A Systematic Review of Cost and Time Efficiency. Business Management and Strategy, 14(2), 220–220. https://doi.org/10.5296/bms.v14i2.21479

Arunthathi S., Logeshwari T., and Anuratha V. 2024. A Research Paper on Online Job Portal System. International Journal of New Innovations in Engineering and Technology, 24(1) 2362-2366

Daoui, A., Mao, H., Yamni, M., Li, Q., Alfarraj, O., & Abd El-Latif, A. A. (2023). Novel Integer Shmaliy Transform and New Multiparametric Piecewise Linear Chaotic Map for Joint Lossless Compression and Encryption of Medical Images in IoMTs. Mathematics, 11(16), 3619. https://doi.org/10.3390/math11163619

Kumar A.N.L, Raju P.L.N, Appaji S.V. and Giri R. (2012). Efficient Design Of Static Analysis Tool For Detecting Web Vulnerabilities. International Journal of Engineering Research and Applications (IJERA) 2(1) pp345-354

Kumar, M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. Procedia Computer Science, 132, 109–117.

Kumar, S., Mahajan, R., Kumar, N., & Khatri, S. K. (2017). A study on web application security and detecting security vulnerabilities. 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 451–455. https://doi.org/10.1109/icrito.2017.8342469

Okediran, O., & Omole, F. (2020). Cybersecurity awareness in Nigerian universities: An exploratory study. Journal of Information Security Research, 8(2), 89–97.

Padwal, H. (2023). A study on importance of job portals in development of urban areas. Our Heritage 67(11) pp 149-153

Robert, W., Denis, A., Thomas, A., Samuel, A., Kabiito, S. P., Morish, Z., & Ali, G. (2024). A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction. Mesopotamian Journal of Artificial Intelligence in Healthcare, 135–169. https://doi.org/10.58496/mjaih/2024/016

Sabrina, F., Sohail, S., & Tariq, U. U. (2024). A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain. Electronics, 13(15), 2962. https://doi.org/10.3390/electronics13152962

Sathiya, T. & Mohanapriya, C. (2025). Online Job Portal. International Research Journal of Modernization in Engineering Technology and Science7(4) (pp. 2582–5208). Retrieved July 3, 2025, from https://www.irjmets.com/uploadedfiles/paper//issue_4_april_2025/73078/final/fin_irjmets1745425836.pdf

Zied H. S. , Abdellatif Ibrahim A. G. , and Salem A. I. (2023). "S-box modification for the block cipher algorithms." Przeglad Elektrotechniczny, 99(4)