ABSTRACT

The widespread use of digital data management in today's information technology era presents new challenges in the field of security, particularly within database systems utilized by various institutions. Threats such as data theft, damage, and misuse—through attacks like SQL Injection and Cross-Site Scripting (XSS)—pose serious risks to sensitive data, making database security a critical concern. To address these issues, a robust security system is required to ensure comprehensive data protection. This study proposes the design of a database security system using a super encryption approach that combines two cryptographic algorithms: Diffie Hellman for key exchange and Blowfish for data encryption and decryption. The system was developed using native PHP and MySQL database and deployed on a web hosting platform. Testing results indicate that the system successfully performs encryption and decryption using a manually implemented Blowfish algorithm. Furthermore, the system effectively safeguards data from SQL Injection attacks by storing the data in ciphertext form. Therefore, this system is considered effective in enhancing data security in web-based database environments.

***Keywords**: Cryptography, Database, Super encryption, Blowfish, Diffie Hellman*