PEFFICIENT PASSWORD-BASED THRESHOLD SINGLE-SIGN-ON AUTHENTICATION

Project Reference No.: *49S_BE_6609*

College : Angadi Institute of Technology and Management, Belagavi
Branch : Department of Computer Science and Engineering
Guide(s) : Prof. Vilas M. Jarali
Student(s) : Mr. Atharv Kolekar
Mr. Niranjan Ingale
Ms. Priyanka Suvarna

Keywords:

Single Sign-On (SSO), Password-Based Security, User Authentication, Data Protection.

Introduction:

The rapid growth of online services has increased the need for secure and efficient authentication systems. Users today access multiple platforms such as websites, applications, and cloud services, which require them to manage multiple usernames and passwords. This creates inconvenience and increases the risk of weak password practices. Single Sign-On (SSO) is an authentication method that allows users to log in once and gain access to multiple services without repeated authentication.

However, traditional SSO systems suffer from security challenges, especially the problem of a single point of failure. If the central authentication server is compromised, all connected services may also be at risk. This highlights the need for a more secure and reliable authentication mechanism. To address these issues, threshold-based authentication techniques have been introduced, where authentication responsibility is distributed across multiple servers.

In this project, an efficient password-based threshold Single Sign-On authentication system is proposed. The system combines the convenience of SSO with the security of distributed authentication. Instead of relying on a single server, the system requires a minimum number of servers to verify a user before granting access. This improves security and ensures that even if some servers are compromised, the system remains protected.

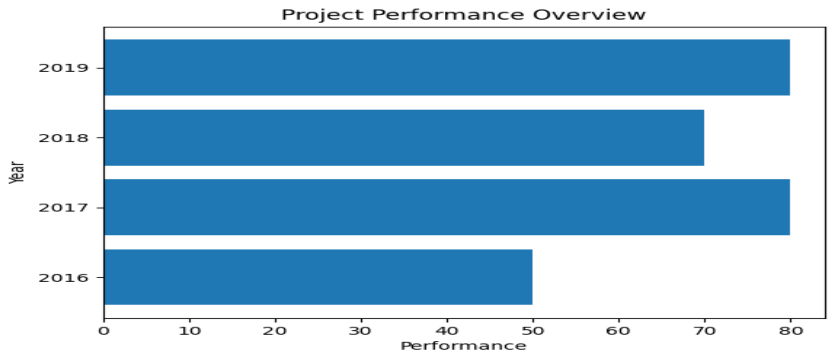

Figure 1: Performance Improvement of SSO Authentication System

Objectives:

1. To develop a secure and efficient password-based Single Sign-On (SSO) authentication system.
2. To enhance security using threshold-based authentication techniques.
3. To enable users to access multiple services with a single login.
4. To reduce risks like password attacks and single point of failure.

Methodology:

1. The methodology of this project focuses on designing and implementing a secure password-based threshold Single Sign-On (SSO) authentication system. The process begins with system design, where the architecture is divided into multiple modules such as user registration, authentication server, service providers, and session management.
2. In the first phase, user registration is carried out, where users create their credentials such as username and password. These credentials are securely stored using encryption techniques to prevent unauthorized access. Proper hashing mechanisms are applied to ensure password safety.
3. In the next phase, multiple authentication servers are set up to implement threshold-based authentication. Instead of relying on a single server, the system distributes authentication responsibility across several servers. A predefined threshold value is set, meaning that a minimum number of servers must validate the user credentials.
4. During the login process, the user enters their credentials once through the SSO interface. The request is then forwarded to multiple authentication servers. Each server independently verifies the credentials and generates a partial authentication response.

Result and Conclusion:

1. The results of the proposed system show that the password-based threshold Single Sign-On (SSO) authentication method provides efficient and secure access to multiple services using a single login. The system successfully reduces the burden of remembering multiple passwords, thereby improving user convenience. During testing, the authentication process was found to be faster and more reliable compared to traditional login systems.
2. The implementation of threshold-based authentication significantly enhanced system security. Since authentication is distributed across multiple servers, the system does not rely on a single point of failure. Even if some servers are compromised, unauthorized access is prevented unless the required threshold is met. This improves resistance against common attacks such as password guessing, replay attacks, and server breaches.
3. The use of encryption and secure session management ensured that user credentials and communication remained protected throughout the process. The system also demonstrated good scalability and can be extended to support multiple services and users efficiently.

References:

[1] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 2025.
[2] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 2024.
[3] A. Zineddine et al., “Single Sign-On Security and Privacy: A Systematic Literature Review,” *Computers, Materials & Continua*, vol. 84, no. 3, pp. 4019–4054, 2025.
[4] M. Joshi, “Single Sign-On Implementation Across Multiple Domain Controllers: Enterprise Architecture Considerations,” *Journal of Computer Science and Technology Studies*, 2025.

Future Scope:

The future scope of this project includes:

1. Integrate advanced multi-factor authentication techniques without using biometrics to enhance security.
2. Improve scalability for cloud-based and large distributed systems.
3. Incorporate AI-based threat detection and stronger encryption for better protection against cyber-attacks.