PROJECT SYNOPSIS

1) Project Reference Number: **46S_BE_3019**

2) Title of the project: PASSWORDLESS AUTHENTICATION SYSTEM USING ZERO KNOWLEDGE PROOFS AND BLOCKCHAIN

3) Name of the College & Department:

- Ramaiah Institute of Technology,
- Computer Science and Engineering

4) Name of the students & Guide(s):

Students:

- M.R.Narasimha Bharadwaj,
- Prajwal S

Guides:

- Dr.Ganeshayya Shidaganti,
- Dr. Annapurna P Patil

5) Keywords:

- Passwordless authentication,
- Zero knowledge proofs,
- Blockchain,
- Security,
- Authentication protocols,
- Elliptic curve cryptography,
- Non-interactive zero knowledge proofs,
- Authentication methods

6) Introduction / Background:

In today's digital world, ensuring secure authentication systems is of paramount importance. Traditional password-based authentication methods have several drawbacks, including vulnerabilities to password breaches and the burden of remembering complex passwords. To address these issues, the project titled "Passwordless Authentication System Using Zero Knowledge Proofs and Blockchain" proposes a novel approach that combines zero knowledge proofs and blockchain technology.

Zero knowledge proofs are cryptographic protocols that allow a party to prove knowledge of certain information without revealing the information itself. This technology has gained significant attention due to its potential for enhancing security and privacy in various domains. The project builds upon the concept of zero knowledge proofs and applies it to the field of authentication.

The project leverages the Elliptic Curve Discrete Logarithm Problem as the foundation for its authentication protocol. By generating a signature using a known value, such as a hashed password, and an elliptic curve's generator point, the project enables the verification of subsequent messages without exposing sensitive information.

The primary objective of this project is to develop a secure and efficient passwordless authentication system. The system aims to provide secure authentication, authorization, and accounting (AAA) operations while maintaining user privacy. By eliminating the need for passwords or hashes, the system mitigates the risks associated with traditional authentication methods.

7) Objectives:

1. To eliminate the use of passwords for authentication and reduce the risk of password-related security breaches.
2. To provide secure and privacy-preserving authentication using zero knowledge proofs.
3. To design a user-friendly and accessible authentication solution that is easy to use and integrate with existing systems.
4. To ensure scalability, cost-effectiveness, and reliability of the authentication system.

8) Methodology:

The project utilizes Python as the primary programming language for implementing the passwordless authentication system. The methodology involves the following steps:

1. **Generation of Signatures:** Generate a signature by multiplying a known value (e.g., hashed password) with the elliptic curve's generator point.
2. **Publication of Signatures:** Publish the generated signature publicly for subsequent message verification without revealing the underlying data.

3. **Authentication Protocol:** Implement a non-interactive zero knowledge proof protocol for authentication. The server generates a random message (token) and requests the user to produce a proof using the provided token. This ensures that the proof cannot be reused in future authentication attempts.
4. **Verification Process:** Verify the proof against the user's public signature. Ensure that the signed data matches the expected value, preventing unauthorized access.
5. **Blockchain Integration:** Explore the integration of blockchain technology to securely store and manage authentication credentials. Utilize the decentralized and immutable nature of blockchain for enhanced security.

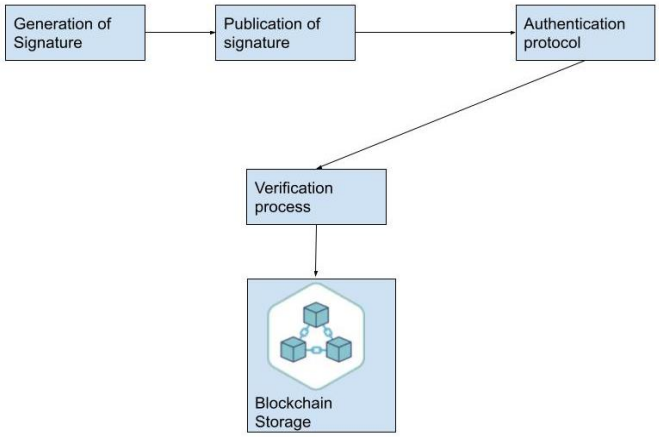

Figure: Architecture Diagram

9) Results and Conclusions:

The implemented passwordless authentication system using zero knowledge proofs and blockchain technology has demonstrated promising results. By utilizing elliptic curve cryptography and non-interactive zero knowledge proofs, the system achieves secure authentication without the need for passwords.

The system ensures that the user's private information remains confidential, as only the necessary verification steps are performed without transmitting sensitive data. The integration of blockchain technology provides an additional layer of security, making it resistant to tampering and unauthorized access.

The results indicate that the proposed system offers robust authentication capabilities while addressing the limitations of traditional password-based methods. The combination of zero knowledge proofs, blockchain, and elliptic

curve cryptography establishes a secure foundation for authentication in various IT and application development industries.

10) Scope for Future Work:

The project opens up several avenues for future research and development. Some potential areas of exploration include:

1. Usability Enhancements: Improve the user experience by developing user-friendly interfaces and seamless integration with existing authentication systems.
2. Scalability and Performance Optimization: Investigate techniques to optimize the system's scalability and performance, allowing for efficient authentication in large-scale applications.
3. Multi-factor Authentication: Extend the system to support multi-factor authentication methods, incorporating additional factors such as biometrics or hardware tokens.
4. Integration with Identity Management Systems: Explore integration possibilities with existing identity management systems to streamline user authentication across multiple platforms.
5. Security Analysis and Threat Modeling: Conduct comprehensive security analysis, including threat modeling and vulnerability assessments, to ensure the system's resilience against emerging threats.

By pursuing these avenues, the passwordless authentication system can continue to evolve, providing enhanced security and convenience for users in a wide range of applications.