ISSN: 2349-6002

A Privacy-Preserving AI-Integrated Blockchain Authentication System Using Zero-Knowledge Proofs

Divyansh Mishra[1], Gourav Kumar[2], Suhani Bhardwaj[3]
[1,2,3]*Department of Computer Applications, Invertis University, Bareilly*
doi.org/10.64643/IJIRTV12I11-207094-459

***Abstract*—In recent years, traditional password-based authentication systems have become increasingly vulnerable to a wide range of cyber threats, including phishing attacks, brute-force attempts, credential stuffing, and large-scale database breaches. These systems typically rely on centralized storage of user credentials, which introduces a single point of failure and significantly increases the risk of sensitive data exposure, even when cryptographic hashing techniques are employed. To overcome these limitations, this paper proposes a novel and privacy-preserving authentication framework that eliminates the need for direct password storage and transmission. The proposed approach leverages a hybrid integration of three advanced technologies: blockchain, zero-knowledge proofs (ZKP), and artificial intelligence (AI), to provide a secure and efficient authentication mechanism. Blockchain technology is utilized to establish a decentralized and tamper-resistant environment for identity verification. By removing dependence on centralized authorities, the system ensures transparency, data integrity, and enhanced security. Furthermore, zero-knowledge proofs enable users to authenticate themselves without revealing their actual credentials, thereby preserving privacy and minimizing the risk of credential leakage during the authentication process. In addition to this, an AI-based anomaly detection module is incorporated to continuously monitor user behavior patterns, such as login time, device information, and geographical location. This intelligent module enables the system to detect suspicious activities in real time and apply adaptive, risk-based authentication strategies to prevent unauthorized access attempts. The proposed hybrid framework significantly enhances system security by eliminating traditional attack vectors associated with password-based systems, while also improving user privacy and overall reliability. Due to its decentralized and intelligent nature, the system is highly suitable for next-generation applications, including Web3 platforms, digital identity management systems, and secure online services.**

***Index Terms*—Artificial Intelligence, Authentication, Blockchain, Cybersecurity, Privacy, Zero-Knowledge Proofs**

I. INTRODUCTION

Authentication is a fundamental aspect of cybersecurity, ensuring that only authorized users can access systems and data. With the rapid increase in internet usage and digital services, authentication systems have become a primary target for cyber attackers. Traditional password-based authentication systems are widely used due to their simplicity, but they suffer from major drawbacks.

Users often create weak passwords or reuse them across multiple platforms, making them vulnerable to attacks. Centralized databases storing user credentials become attractive targets for hackers. Even advanced techniques such as hashing and encryption cannot fully eliminate risks, as attackers can use sophisticated methods to crack passwords. Moreover, traditional systems lack intelligent mechanisms to detect unusual user behavior, making them ineffective against modern threats.

To overcome these challenges, there is a need for a secure, decentralized, and intelligent authentication system. Blockchain technology provides a decentralized and tamper-resistant framework for secure authentication [1],[3], while Zero-Knowledge Proofs (ZKPs) enable users to prove their identity without revealing sensitive information, thereby enhancing privacy [2],[4]. Furthermore, Artificial Intelligence (AI) can intelligently monitor user behavior and detect anomalous activities, strengthening the overall security of authentication systems [5].

This paper proposes a hybrid approach that combines blockchain, zero-knowledge proofs, and artificial intelligence. The system ensures privacy, eliminates

password storage, and introduces intelligent monitoring, making it a robust and future-ready authentication solution.

II. LITERATURE REVIEW

In recent years, researchers have explored various approaches to improve authentication systems by incorporating advanced technologies such as blockchain, cryptographic protocols, and artificial intelligence. This section reviews the existing work in these domains and highlights their limitations.

Several studies have proposed blockchain-based authentication systems to address the issue of centralization. Blockchain technology provides a decentralized and tamper-resistant environment where authentication data can be stored securely. Researchers have demonstrated that blockchain eliminates the need for a central authority and reduces the risk of single-point failures [1],[3]. However, most blockchain-based authentication systems lack strong privacy mechanisms. Since blockchain data is often publicly accessible, sensitive metadata related to user identity may still be exposed, leading to potential privacy concerns [9].

Another line of research focuses on zero-knowledge proof (ZKP)-based authentication systems. ZKP allows a user to prove knowledge of a secret (such as a password) without revealing the secret itself [2]. This approach significantly enhances privacy and reduces the risk of credential leakage during transmission. Various protocols, including zk-SNARKs and zk-STARKs, have been developed to implement efficient zero-knowledge proofs [4]. Despite their advantages, ZKP-based systems often involve high computational complexity and do not incorporate mechanisms to detect suspicious or anomalous user behavior.

In addition, artificial intelligence (AI)-based authentication and security systems have gained popularity in recent years. AI techniques, particularly machine learning algorithms, are used to analyze user behavior patterns such as login time, device information, IP address, and location. These systems can effectively detect anomalies and potential intrusions in real time [5]. However, most AI-based systems are implemented in centralized environments and rely on traditional authentication mechanisms, which limits their overall effectiveness in ensuring privacy and decentralization.

Some hybrid approaches have attempted to combine two of these technologies. For instance, blockchain with AI has been used for secure data management and threat detection [10], [11] while ZKP with blockchain has been explored for privacy-preserving transactions [4]. However, these approaches still lack a complete integration of blockchain, zero-knowledge proofs, and AI within a unified authentication framework.

Fig.1 shows the comparison of existing systems for privacy preserving using ZKPs.

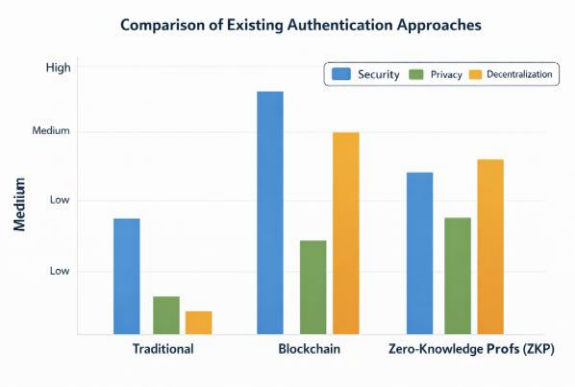

Fig.1: Comparisons of Existing Authentication Approaches

Therefore, despite significant advancements in individual domains, there remains a research gap in designing a comprehensive authentication system that simultaneously ensures decentralization, privacy preservation, and intelligent threat detection. This gap motivates the proposed system, which integrates blockchain, ZKP, and AI to provide a secure, privacy-preserving, and adaptive authentication solution

III. PROBLEM STATEMENT

In the contemporary digital ecosystem, authentication mechanisms serve as the primary gateway for securing user identities and sensitive information. However, most existing systems rely on traditional password-based authentication, which has proven to be increasingly inadequate in addressing modern cybersecurity challenges.

One of the fundamental issues with current authentication systems is their dependence on centralized storage of user credentials. This architecture introduces a critical vulnerability known as a *single point of failure*, where a successful breach of the central database can compromise the credentials

of millions of users simultaneously. Despite the use of hashing and encryption techniques, attackers continue to exploit weaknesses through advanced methods such as brute-force attacks, dictionary attacks, and credential stuffing [7].

Furthermore, traditional systems lack privacy-preserving capabilities, as user credentials are either stored or transmitted during the authentication process. This increases the risk of interception, unauthorized access, and data leakage. In addition, these systems do not incorporate intelligent mechanisms to monitor user behavior, making them incapable of detecting anomalous or suspicious login activities in real time.

Another critical limitation is the absence of decentralization, which restricts transparency and increases dependency on trusted third parties. This not only affects system reliability but also raises concerns regarding data ownership and control.

Although emerging technologies such as blockchain, zero-knowledge proofs, and artificial intelligence have individually demonstrated potential in enhancing security and privacy, there is still a lack of a unified framework that integrates these technologies into a single, cohesive authentication system.

Therefore, there exists a pressing need for a next-generation authentication solution that is secure, decentralized, privacy-preserving, and intelligent, capable of overcoming the limitations of traditional systems while addressing the evolving landscape of cyber threats.

IV. PROPOSED SYSTEM

To address the limitations of traditional authentication mechanisms, this research proposes a hybrid, privacy-preserving authentication framework that integrates Blockchain Technology, Zero-Knowledge Proofs (ZKP), and Artificial Intelligence (AI). The objective of the proposed system is to eliminate password dependency, enhance data privacy, and provide intelligent threat detection within a decentralized environment [6],[8].

Unlike conventional systems that rely on direct password transmission and centralized storage, the proposed approach enables users to authenticate themselves using cryptographic proofs, ensuring that sensitive credentials are never exposed during the authentication process

A.System Overview

The proposed system is composed of four major components:

- User Interface Layer (Client Side)
- Zero-Knowledge Proof (ZKP) Module
- Blockchain Network (Smart Contract Layer)
- AI-Based Anomaly Detection Module

Each component plays a critical role in ensuring secure, private, and efficient authentication.

B.System Architecture Description

In this architecture, the user initiates the authentication process through a client interface. Instead of submitting a password, the system generates a Zero-Knowledge Proof (ZKP) based on the user's secret credentials. This proof is then transmitted to the blockchain network, where it is verified using smart contracts [5], [12].

Simultaneously, the AI module analyzes contextual and behavioral parameters such as login time, device information, IP address, and geographical location. Based on this analysis, the system assigns a risk score to the login attempt.

The final authentication decision is made by combining:

- Cryptographic verification (ZKP + Blockchain)
- Behavioral analysis (AI module)

Fig.2 Shows the whole system Architecture for decision making.

Only when both conditions are satisfied is access granted.

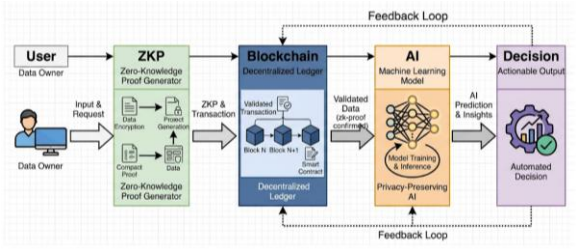

Fig.2: System Architecture Diagram

V. SYSTEM MODEL

The proposed authentication framework is modeled as a secure, decentralized, and privacy-preserving system that combines cryptographic verification with intelligent decision-making. The system ensures that authentication is granted only when both identity verification and behavioral validation are successfully satisfied.

A. *System Entities*

The system consists of the following key entities:

- User(U): An entity attempting to access the system by proving its identity.
- Secret Credential(S): A private value (password or key) known only to the user.
- Zero-Knowledge Proof(P): A cryptographic proof generated by the user to validate knowledge of the secret without revealing it.
- Blockchain Network(B): A decentralized ledger responsible for storing commitments and verifying proofs through smart contracts.
- AI Model(M): A machine learning-based module used to analyze user behavior and detect anomalies.
- Risk Score(R): A numerical value generated by the AI model representing the likelihood of suspicious activity.
- Threshold(T): A predefined limit used to classify behavior as normal or suspicious.

B. *Mathematical Representation*

The authentication process can be formally defined as follows:

Let:

- $U \rightarrow S$: User possesses a secret
- $P = ZKP(S)$: Proof generated from the secret
- $Verify(P, B) \in \{True, False\}$: Blockchain verification function
- $R = M(X)$: Risk score computed from behavioral data X

Authentication Condition

Authentication is successful if and only if:

Verify (P, B) = True ∧ R < T

Where:

- Verify (P, B) ensures correctness of the proof
- $R < T$ ensures that user behavior is within acceptable limits

C. *Behavioral Feature Model*

The AI module evaluates user behavior using a feature vector:

X = {IP, Device, Location, Time}

The model computes:

R = f(X)

Where:

- f is a trained machine learning function
- $R \in [0,1]$, where higher values indicate higher risk

D. *System Workflow Model*

The system operates as a sequence of transformations:

S → P → Verify(P) → X → R → Decision

Where:

- Secret is transformed into proof
- Proof is verified
- Behavior is analyzed
- Final decision is generated

E. *Decision Function*

The final authentication decision can be expressed as:

D = {Access Granted, If Verify(P) = True AND R < T

{Access Denied, otherwise

All Working Models can be shown using Fig.3.

VI. ALGORITHM

The proposed authentication system follows a multi-layered algorithmic approach that integrates Zero-Knowledge Proof (ZKP) for secure identity verification, blockchain for decentralized validation, and Artificial Intelligence (AI) for behavioral risk assessment.

The algorithm is divided into two major phases: Registration Phase and Authentication Phase, followed by a Decision Mechanism.

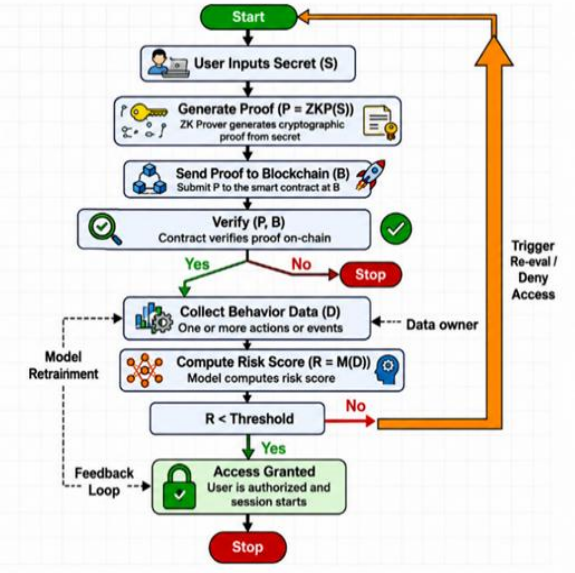

Fig.3: Working Algorithm

A. *Notations Used*

Let:

U→ User

S→ Secret credential

$C = Hash(S)$→ Cryptographic commitment
P→ Zero-Knowledge Proof
B→ Blockchain network
M→ AI model
X→ Behavioral feature vector
R→ Risk score
T→ Risk threshold
D→ Final decision

B. *Algorithm 1: Registration Phase*
Input: User secret S
Output: Stored commitment on blockchain

Steps:
1. User selects secret credential S
2. Compute cryptographic commitment: C ← Hash(S)
3. Generate Zero-Knowledge Proof: P ← ZKP (S, C)
4. Deploy smart contract on blockchain B
5. Store commitment C (or proof-related parameters) on B
6. Return Registration Success

C. *Algorithm 2: Authentication Phase*
Input: User secret S
Output: Verification status
1. User inputs credential S
2. Generate fresh proof: P' ← ZKP(S)
3. Send proof P' to blockchain B
4. Blockchain executes smart contract: V ← Verify (P', C)
5. IF V = False THEN
Return Access Denied
ELSE
Proceed to AI Risk Evaluation

D. *Algorithm 3: AI-Based Risk Evaluation*
Input: Behavioral data X
Output: Risk score R
1. Collect behavioral features:
X ← {IP, Device, Location, Time}
2. Input X into trained AI model M
3. Compute risk score:
R ← M(X)
4. Normalize R within range [0,1]

E. *Algorithm 4: Decision Making Mechanism*
Input: Verification result V, Risk score R
Output: Final decision D
1. IF (V = True) AND (R < T) THEN
D ← Access Granted
2. ELSE IF (V = True) AND (R ≥ T) THEN
D ← Trigger Multi-Factor Authentication (MFA)
3. ELSE
D ← Access Denied
4. Return D

F. *Combined Algorithm (End-to-End)*
BEGIN
1. User inputs credentials S
2. Generate ZKP proof P'
3. Send P' to blockchain
4. V ← Verify (P', C)
5. IF V = False THEN
Deny Access
ELSE
X ← Collect behavior data
R ← Compute risk score
IF R < T THEN
Grant Access
ELSE
Trigger MFA / Deny Access
ENDIF
ENDIF
END
The combined working of all the algorithms in the systems is demonstrated using Fig.4.

VII. IMPLEMENTATION

The proposed authentication system is implemented using a multi-layered architecture that integrates web technologies, blockchain, and artificial intelligence. The frontend is developed using React.js, which provides an interactive user interface for registration and login. The backend is built using Node.js and Express.js, responsible for handling API requests, generating Zero-Knowledge Proofs (ZKP), and coordinating communication between different system components. The blockchain layer is implemented using the Ethereum platform, where smart contracts written in Solidity are used to store cryptographic commitments and verify ZKP proofs [4],[9]. This ensures decentralized and tamper-resistant authentication. The ZKP mechanism is implemented using tools such as Circom and SnarkJS, which enable secure proof generation and verification without revealing user credentials.Fig.5 shows the system architecture with the integration of AI Module Layer.

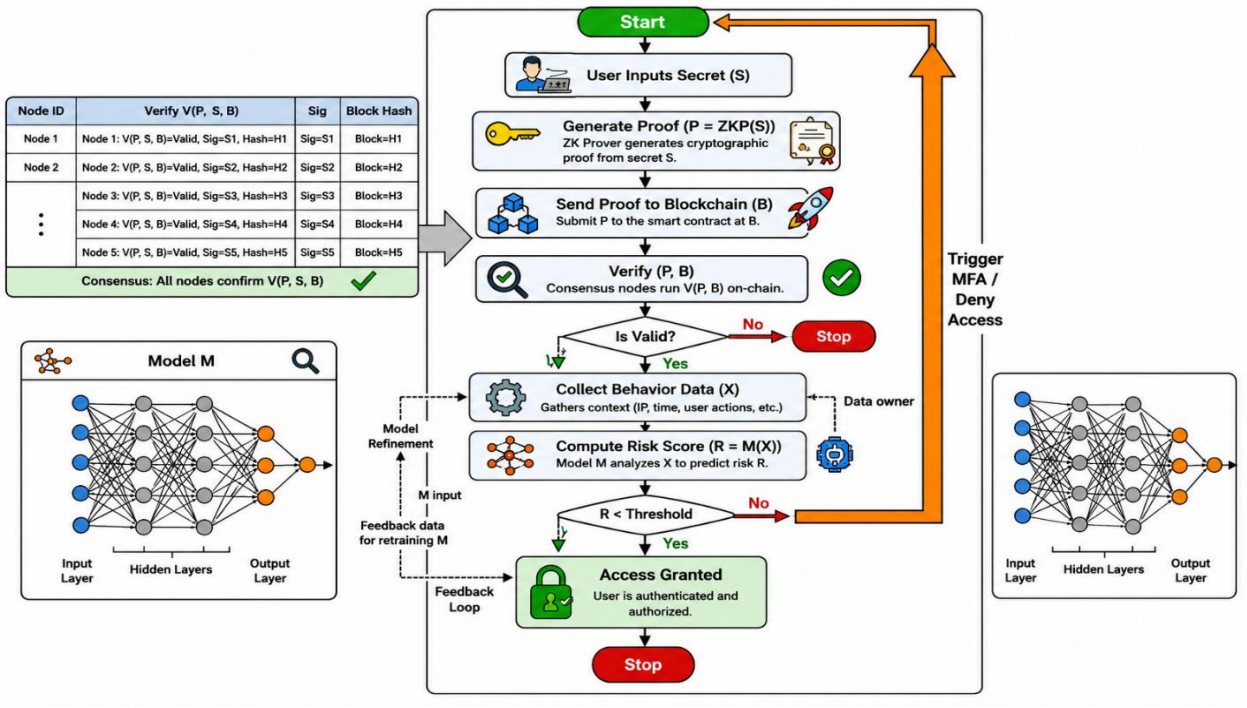

Fig.4: Working Architecture Using ZKPs

The AI-based anomaly detection module is developed using Python and machine learning libraries, where user behavior (such as IP address, device, location, and login time) is analyzed to generate a risk score. This score is used to detect suspicious activities and enhance security. The overall system ensures secure communication through HTTPS, eliminates password storage, and provides a scalable and efficient authentication framework [13].

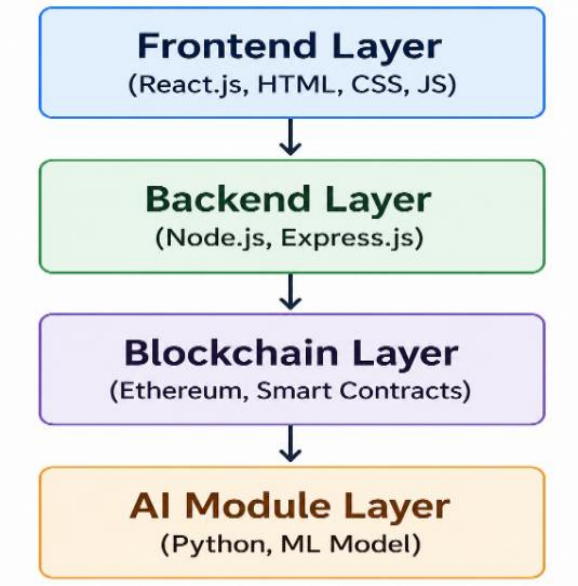

Fig5: Overall System Structure

VIII. RESULT AND ANALYSIS

The proposed authentication system was evaluated based on key parameters such as security, privacy, and resistance to cyber-attacks. Compared to traditional password-based systems, the proposed model demonstrates significant improvements. Since no passwords are stored or transmitted, the risk of data breaches and credential leakage is greatly reduced.

The integration of Zero-Knowledge Proofs ensures secure authentication, while blockchain provides decentralization and data integrity. Additionally, the AI module successfully detects suspicious login attempts by analyzing user behavior, thereby enhancing overall system security. These results indicate that the proposed system is more secure, privacy-preserving, and reliable than conventional authentication mechanisms.

IX. SECURITY ANALYSIS

The security of the proposed authentication system is achieved through a multi-layered defense mechanism that combines cryptographic techniques, decentralized infrastructure, and intelligent monitoring. This layered

approach ensures strong protection against a wide range of cyber threats.

A.Cryptographic Security (ZKP Layer)

The use of Zero-Knowledge Proofs (ZKP) ensures that authentication is performed without revealing the user's secret credential. This provides the following guarantees:

- Zero-Knowledge Property: No information about the secret is exposed
- Completeness: Legitimate users are always authenticated
- Soundness: Attackers cannot forge valid proofs

Since each authentication generates a new proof, the system prevents replay attacks and ensures forward security.

B.Blockchain Security

The blockchain layer enhances system security through decentralization and immutability:

- Decentralization: Eliminates single point of failure
- Immutability: Stored data cannot be altered or deleted
- Transparency: Verification process is auditable Smart contracts ensure that proof verification is performed securely and consistently across the network.

C. AI-Based Security

The AI module adds an intelligent security layer by analyzing user behavior:

- Detects anomalies in login patterns
- Identifies suspicious activities in real time
- Assigns risk scores for adaptive authentication

This enables the system to prevent unauthorized access even if cryptographic verification is bypassed.

D. Resistance to Common Attacks

The proposed system is resistant to the following attacks:

- Phishing Attacks: No password is shared or exposed
- Brute-force Attacks: No password storage makes attacks ineffective
- Credential Stuffing: Credentials are never reused or transmitted
- Replay Attacks: Fresh ZKP proof for each session
- Database Breaches: No sensitive data stored in plaintext

ZKP Layer → Blockchain Layer → AI Layer

Fig.6 shows the Security Layer Architecture The system follows a layered security approach:

X. ADVANTAGES

The integration of Zero-Knowledge Proofs, blockchain technology, and artificial intelligence provides a highly secure authentication framework. The strong security of the proposed system offers several significant advantages over traditional authentication mechanisms.

A. Enhanced Data Confidentiality

The system ensures that user credentials are never stored or transmitted in plaintext form. By using Zero-Knowledge Proofs, users can authenticate themselves without revealing their actual secrets, thereby maintaining strict confidentiality of sensitive information.

B. Elimination of Credential Leakage

Traditional systems are prone to data breaches due to centralized storage of passwords. In contrast, the proposed system eliminates password storage entirely, reducing the risk of credential theft and unauthorized access.

C. Enhanced Data Confidentiality

The system ensures that user credentials are never stored or transmitted in plaintext form. By using Zero-Knowledge Proofs, users can authenticate themselves without revealing their actual secrets, thereby maintaining strict confidentiality of sensitive information.

D. Elimination of Credential Leakage

Traditional systems are prone to data breaches due to centralized storage of passwords. In contrast, the proposed system eliminates password storage entirely, reducing the risk of credential theft and unauthorized access.

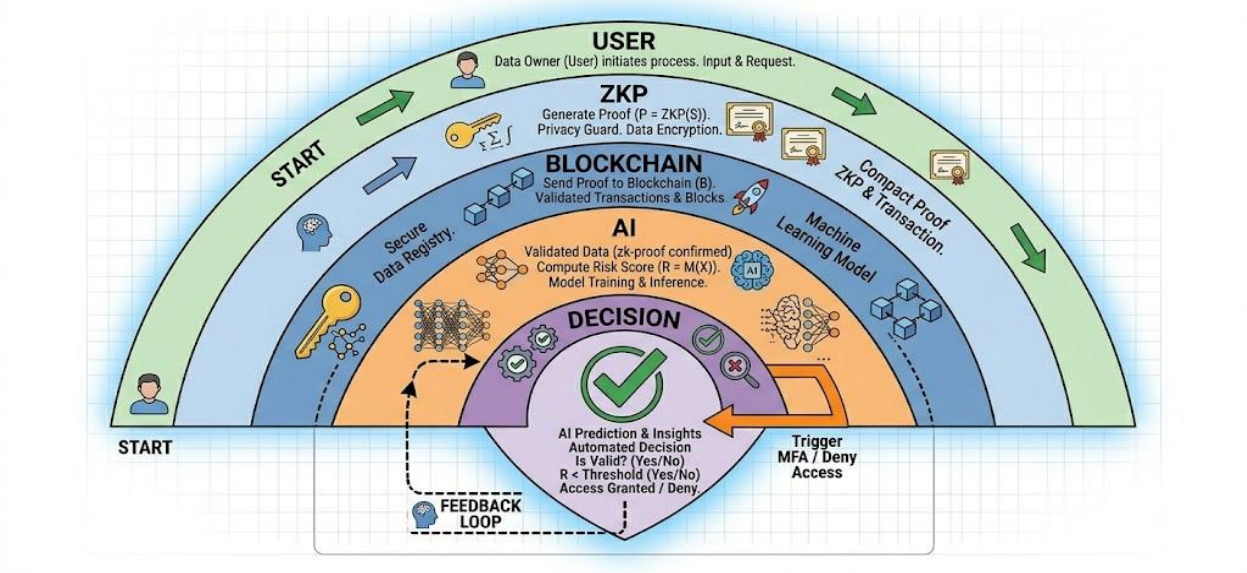

Fig.6: Security Layers Diagram

E. Resistance to Common Cyber Attacks

The strong security design makes the system highly resistant to various cyber threats, including:

- Phishing attacks
- Brute-force attacks
- Credential stuffing
- Replay attacks

This significantly reduces the chances of successful attacks.

F. Decentralized Trust Model

By leveraging blockchain technology, the system removes dependence on centralized authorities. This decentralization eliminates the single point of failure and enhances overall system reliability and trustworthiness.

G. Tamper-Proof Data Integrity

Blockchain ensures that stored data cannot be altered or manipulated. This guarantees the integrity of authentication records and prevents unauthorized modifications.

H. Intelligent Threat Detection

The integration of AI enables real-time monitoring of user behavior.

Suspicious activities are detected instantly, allowing the system to take proactive security measures such as denying access or triggering multi-factor authentication.

I. Adaptive and Context-Aware Security

Unlike static authentication systems, the proposed model adapts based on user behavior and risk levels. This dynamic approach improves both security and usability.

J. Improved User Privacy

Since no sensitive information is exposed during authentication, the system ensures a high level of privacy protection, which is critical in modern digital environments.

K. I Future-Ready Security Architecture

The system is designed to meet the requirements of next-generation applications such as Web3, decentralized identity systems, and secure cloud platforms, making it scalable and future-proof.

XI. CONCLUSION & FUTURE SCOPE

The proposed authentication system can be further enhanced by integrating more efficient and lightweight Zero-Knowledge Proof protocols to reduce computational overhead. Future research can focus on incorporating advanced AI models, such as deep learning techniques, to improve the accuracy of anomaly detection. The system can also be extended by integrating biometric authentication methods for multi-factor security. Additionally, the use of private or hybrid blockchain networks may improve

scalability and reduce latency. Exploring quantum-resistant cryptographic techniques can further strengthen the system against future security threats.

This paper presented a secure and privacy-preserving authentication framework by integrating Zero-Knowledge Proofs, blockchain technology, and artificial intelligence. The proposed system eliminates the need for password storage, enhances data privacy, and provides decentralized and tamper-resistant verification. Additionally, the AI-based anomaly detection mechanism strengthens security by identifying suspicious activities in real time.

Overall, the system effectively addresses the limitations of traditional authentication methods and offers a robust, scalable, and future-ready solution for modern digital applications.

REFERENCES

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

[2] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM Journal on Computing, vol. 18, no. 1, pp. 186–208, Feb. 1989.

[3] V. Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014.

[4] E. Ben-Sasson et al., "Succinct non-interactive zero knowledge for a von Neumann architecture," in Proc. 23rd USENIX Security Symposium (USENIX Security '14), San Diego, CA, USA, Aug. 2014, pp. 781–796.

[5] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[6] J. Groth, "On the size of pairing-based non-interactive arguments," in Advances in Cryptology – EUROCRYPT 2016, Lecture Notes in Computer Science, vol. 9666. Berlin, Germany: Springer, 2016, pp. 305–326.

[7] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin," in Proc. IEEE Symp. Security and Privacy, 2014.

[8] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "SNARKs for C: Verifying program executions succinctly and in zero knowledge," in Advances in Cryptology – CRYPTO 2013, Lecture Notes in Computer Science, vol. 8042. Berlin, Germany: Springer, 2013, pp. 90–108.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557–564.

[10] G. Rautela, B. Sharma, A. Kumar, R. Saxena, and A. Sanghi, "Exploring the transformative role of blockchain in healthcare data protection and supply chain transparency," GRENZE International Journal of Engineering and Technology, vol. 10, no. 1, pp. 2558–2564, 2024.

[11] R. Agarwal, P. K. Agarwal, B. Parihar, V. Sharma, and A. Sanghi, "Enhancing blockchain financial security through DB-BOA optimization and ADTCN frameworks," in Proc. 2025 IEEE 7th Int. Conf. Computing, Communication and Automation (ICCCA), Greater Noida, India, 2025, pp. 1–6, doi: 10.1109/ICCCA66364.2025.11325619.

[12] R. Agarwal, A. Sanghi, P. Vishwakarma, and G. Agarwal, "Blockchain security: A comprehensive review of current threats and solutions," in Proc. 16th Int. Conf. Advances in Computing, Control, and Telecommunication Technologies (ACT), vol. 1, 2025, pp. 4951–4957.

[13] G. Rautela, B. Sharma, A. Kumar, R. Saxena, and A. Sanghi, "Exploring the transformative role of blockchain in healthcare data protection and supply chain transparency," Grenze International Journal of *Engineering & Technology (GIJET)*, vol. 12, no. 2, pp. 2769–2776, 2026.