

Recent Advances in Blockchain-Based Identity and Access Management for Cybersecurity

Mr. Raman Kumar

Assistant Professor, Department of Computer Science and Applications Mandsaur(M.P.) 458001

ABSTRACT: The rapid expansion of digital services, cloud computing, IoT, and interconnected platforms has increased the need for secure and privacy-preserving Identity and Access Management (IAM). Traditional centralized and federated IAM systems face challenges including single points of failure, privacy risks, limited user control, interoperability issues, and identity-based cyberattacks. This paper reviews recent advances in blockchain-based IAM for cybersecurity, focusing on blockchain architectures, Self-Sovereign Identity (SSI), decentralized identifiers (DIDs), smart contracts, authentication mechanisms, federated identity, and AI-integrated IAM. The review demonstrates that blockchain can provide decentralized, tamper-resistant, transparent, and auditable identity management, while SSI enables greater user ownership and control over digital identities. Smart contracts support automated authentication and access control, whereas AI integration enables anomaly detection, behavioural analysis, adaptive authorization, and intelligent threat mitigation. The reviewed studies also indicate improvements in privacy, credential verification, trust, and resistance to identity-related threats. However, scalability, interoperability, computational overhead, secure key management, privacy, and regulatory compliance remain significant challenges. Overall, blockchain-based IAM provides a promising foundation for secure, resilient, privacy-preserving, and user-centric cybersecurity environments.

KEYWORDS: Blockchain, Identity and Access Management (IAM), Cybersecurity, Authentication, Decentralized Identity, Single Sign-On (SSO), Self-Sovereign Identity (SSI).

I. INTRODUCTION

Cybersecurity is essential in today's networked planet to protect data, networks, and dossiers from unauthorized access, criminal activity, and potential instabilities. The demand for efficient cybersecurity measures has never been greater due to the technology's exponential growth and growing reliance on digital infrastructure. Even contemporary technologies such as cloud computing, mobile computing, net investment, and e-commerce demand an extreme level of security [1]. Since these electronics involve some important facts about a person, their freedom has become a top priority. Each country's safety and financial well-being depend on enhancing cyber safety and protecting vital information infrastructure. For a society to efficiently put an end to or recover from cyberattacks, all of the arrangements, society, and tools must agree. The tasks of finding, inspection, and remediation are three important freedom processes that can be increased by a united threat administration whole [2].

This has been conducted to highlight IAM's significance, advantages, and disadvantages. It has been noticed that "Google", "Facebook", "GitHub", and other well-known web-based organisations provide free authentication opportunities that can be easily coordinated through online applications. 'Key Cloak' is an open-source IAM that focuses on current administrations and applications designed to provide a keyguard for application protections and administrations [3]. 'Azure ATP (Advanced Threat Protection)' is a completely cloud-based

solution that helps investigate and detect any type of security incidents across the entire network system. It assists in securing any organization from compromised identities and insider threats. It has the ability to identify threat patterns along with their resources within the cloud and on-premises [4].

IAM has been defined as the "security discipline that enables the right individuals to access the right resources at the right times for the right reasons." It is a critical aspect of security for

both businesses and individuals, although the implementation of IAM solutions has not been smooth. Traditional forms of IAM are often siloed solutions, for example, single sign-on (SSO), federated ID, and password management. These solutions mean more methods of proving and verifying identity while often creating duplicate or conflicting forms of digital identity [5]. In this context, blockchain technology has emerged as a promising approach for improving identity and access management by providing a decentralized, distributed, and tamper-resistant framework for managing identity information and access permissions [6]. Blockchain-based IAM can reduce dependence on centralized authorities, enhance transparency and auditability, and provide users with greater control over their digital identities.

Identity Management Systems (IDMSs), defined by NIST as systems or applications that manage identity proofing, registration, verification, and issuance, are traditionally deployed using centralized or federated architectures, but both approaches struggle to address evolving security, privacy, and interoperability requirements effectively [7]. Centralized IDMSs

suffer from inherent risks such as single points of failure, limiting scalability across multi-organizational environments and providing users with minimal control over their personal identity data [8]. Federated IDMSs address several critical limitations of centralized architectures by eliminating single points of failure, strengthening user autonomy over identity data, and enabling secure cross-domain authentication and access. However, they remain vulnerable to privacy breaches during inter-organizational data exchange, lack full support for holistic identity lifecycle management, and face persistent interoperability constraints across heterogeneous systems [9].

A. Structure of the Paper

This paper is organized as follows: Section II introduces Identity and Access Management in Cybersecurity. Section III explores Blockchain-Based Identity and Access Management. Section IV reviews recent literature, and Section V concludes the paper while outlining potential future research directions.

II. IDENTITY AND ACCESS MANAGEMENT IN CYBERSECURITY

Identity in the modern era is increasingly dependent on the Internet, especially with regard to information, forums, social networking sites, games and the applications it provides [10]. This has resulted in an increasing demand for privacy rights that protect the creation of a virtual identity without hindrance, especially with the increasing number of people who make up their identity on the Internet, and this would better protect the independent and unimpaired development of virtual identity in cyberspace, recognizing virtual identities as separate assets and allocating Virtual privacy rights provides an opportunity to organize cyberspace, in an innovative way [11].

A. The Role of Identity and Access Management in Cybersecurity

In the modern digital ecosystem, Identity and Access Management (IAM) has become a critical pillar in any organization’s cybersecurity strategy. As organizations face increasing regulatory pressures and sophisticated cyber threats, the role of IAM in ensuring compliance with cybersecurity frameworks is more important than ever. At its core, IAM governs the lifecycle of user identities and their access to organizational resources, ensuring that only authorized individuals can interact with sensitive data and critical systems [12]. However, IAM goes beyond merely securing access; it plays a central role in ensuring compliance with a variety of legal, industry-specific, and international regulations designed to protect data, uphold privacy, and safeguard systems against breaches.

B. Fundamentals of Identity and Access Management

Identity and Access Management (IAM) is a cybersecurity framework that ensures authorized users access appropriate resources at the right time. It manages digital identities through authentication, authorization, and lifecycle management, thereby improving data protection, reducing unauthorized access, and supporting regulatory compliance.

- **Digital Identity:** Represents the online form of a person's physical identity and enables individuals to be uniquely recognized within digital environments [13].
- **Authentication:** Confirms a user's claimed identity using knowledge-based methods such as passwords [14], possession-based methods such as tokens or smart devices, and inherence-based methods such as biometrics.
- **Authorization:** Determines whether an authenticated user has permission to access a resource or perform a specific action, based on defined access policies [15].
- **Identity Lifecycle:** Manages an identity throughout its lifecycle, from creation and assignment of accounts and permissions to modification and eventual deactivation [16]. It supports both workforce and customer identities while enabling secure digital transactions

C. Traditional IAM Models

Traditional IAM models use centralized identity repositories and predefined access control policies to authenticate users and manage access to organizational resources. Although effective in conventional IT environments, they face challenges in supporting dynamic, cloud-based, and distributed systems.

- **Centralized IAM:** Centralized identity management systems (CIMSs), also referred to as traditional identity management systems, are commonly implemented in environments where a single entity manages all user identity-related tasks. As shown in Fig 1, this entity is called an identity provider (IdP) and is responsible for storing credentials and handling authentication requests.

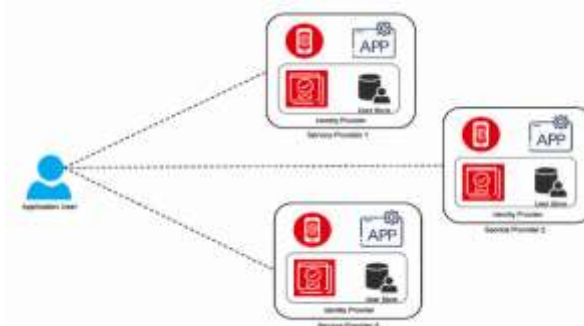


Fig. 1. Centralized Identity Management Systems

- **Federated Identity Management:** In FIM, each organization has its own IdP to share resources and authenticate users across domains [7]. This model allows interoperability between organizations while retaining the centralized nature of identity management, as shown in Fig 2.

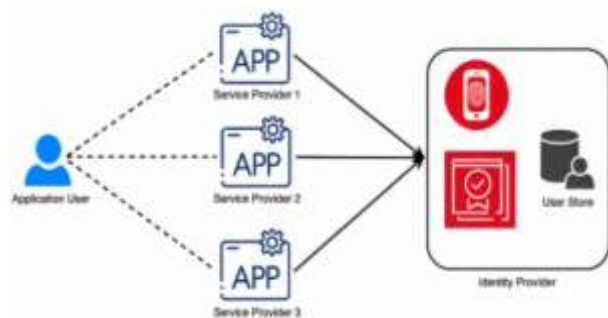


Fig. 2. Federated Identity Management

- **Single Sign-On (SSO):** SSO is a feature that allows users to log in once to a system and gain access to multiple trusted services, without the need to authenticate again. It enhances user experience by reducing the number of times the user needs to log in and validate their identity. The central authority manages user identity authentication and issues a token that grants access to different services, as shown in Fig 3.

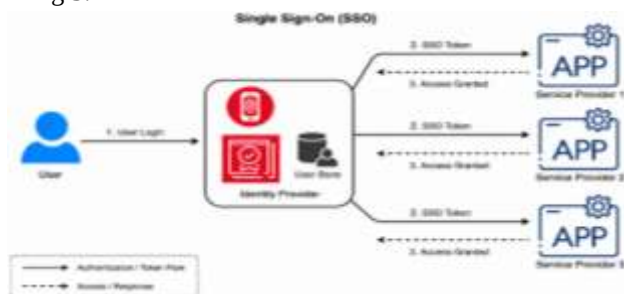


Fig. 3. Single Sign-on (Sso)

D. IAM Threat Landscape

Understanding IAM's defensive role requires understanding the adversarial context within which it operates. Threat actors systematically target identity infrastructure because compromising identity controls yields disproportionate access relative to the effort of attacking individual systems or applications.

- **Credential Theft and Abuse:** Credential-based attacks phishing, credential stuffing, password spraying, and adversary-in-the-middle (AiTM) proxy attacks, are the most prevalent initial access vectors observed in enterprise breach investigations.
- **Privilege Escalation:** Once initial access is achieved, sophisticated threat actors pursue privilege escalation to obtain the elevated permissions necessary for their ultimate objectives.
- **Insider Threats:** Insider threats, whether malicious, negligent, or resulting from compromised credentials, pose a fundamentally distinct challenge because the perpetrating identity is authenticated and operating within its assigned permissions.
- **Non-Human Identity Threats:** The proliferation of service accounts, API keys, OAuth tokens, and machine identities has created an expansive and often poorly governed attack surface [17][18].

III. BLOCKCHAIN-BASED IDENTITY AND ACCESS MANAGEMENT

It is a ledger technology capable of storing data that utilizes a decentralized design that is dependable and prevents tampering of data. A decentralized computing and information sharing platform that allows various authoritative domains that do not trust each other to cooperate, coordinate, and participate in rational decision-making [19]. Blockchain technology ensures that local copies are consistent. Local copies are identical at each node and are always updated based on global information.

A. Types of Blockchain for IAM

Blockchain solutions can be deployed using a variety of permission and access control techniques. There are four types of blockchain schemes: public, private, hybrid, and consortium. The different blockchain types are depicted in Fig 4.



Fig. 4. Types of Blockchai

- **Public Blockchain:** A permissionless network that is open to everyone, allowing anyone to join and participate [20]. Blockchain-based identification and authentication systems commonly use Ethereum, Bitcoin, and Litecoin. It is immutable and decentralized, and primarily supports cryptocurrency exchange and mining.
- **Private Blockchain:** A permission-based network operating within a restricted environment and controlled by a particular organization [21]. Access is provided by invitation and requires authorization from the governing body.
- **Hybrid Blockchain:** Combines private and public blockchain components, allowing organizations to maintain private and public systems. Smart contracts regulate data access and determine which information is made public, while transactions remain unchangeable.
- **Consortium Blockchain:** A federated network in which multiple organizational members collaboratively control the consensus process. It combines features of public and private blockchains, with multiple authorities responsible for network governance.

B. Key Characteristics of Blockchain

Blockchain is characterized by decentralization, Persistency, anonymity, and auditability, which ensure secure and tamper-resistant data management. These features enhance trust among participants, eliminate single points of failure, and provide

reliable identity and access management for cybersecurity applications.

- **Decentralization:** Blockchain operates on a distributed network where no single entity holds control. Instead of relying on a central authority, decisions are made collectively by all participating nodes, enhancing security and reducing the risk of centralized control or failures.
- **Persistence:** Once a transaction is recorded on the blockchain, it is permanent and unchangeable [22]. This ensures data integrity, as the records cannot be altered or deleted, making the system highly reliable for keeping historical information.
- **Anonymity:** Blockchain allows users to conduct transactions without revealing their real identities. Participants are identified through cryptographic addresses, ensuring privacy while still maintaining trust in the system.
- **Auditability:** The blockchain's transparent and chronological record of all transactions makes it easy to track and verify data. This auditability ensures that every transaction can be traced back to its origin, promoting transparency and trustworthiness in the network.

C. Blockchain Layered Architecture

This section covers the layered architecture of blockchain. From top to bottom, the blockchain structure is divided into the Application layer, Consensus layer, Network layer, Data layer and Hardware Layer.

- **Hardware/Infrastructure Layer:** Blockchain is a distributed system of computers connected in a peer-to-peer manner that computes transactions, approves them, and stores them in shared database in an ordered 246 structure. Every device within a blockchain network is called a node. The duty of nodes is to validate the transactions, organize them into blocks, and further broadcast them to the blockchain network.
- **Data Layer:** This section is concerned with the transactions which are arranged in blocks, and placed in a peer-to-peer network. The data structure of blockchain can be represented in the form of linked list, which is ordered. It consists of two primary components pointers and a linked list [23]. The pointers are variables, whose value is the address of another variable, and linked list is a linear collection of blocks, where each block has data and pointers to the previous block.
- **Network Layer:** The network layer, is responsible for peer-to-peer communication between nodes. Its main functions are discovery of neighbouring nodes that can communicate, making transactions, and propagating the block of transactions. A peer-to-peer network is a computer network in which devices are distributed and share the network's workload to achieve a common goal. Nodes perform transactions on the blockchain.

- **Consensus Layer:** The consensus layer is the very basic and important layer for any blockchain (Ethereum, Hyperledger, or any other). The consensus protocol ensures the stable working of blockchain technology [24]. Behind every blockchain, there is a consensus algorithm. Consensus is responsible for validating the transactions, maintaining the order, and ensuring every block agrees on it. It ensures that power remains circulating and decentralized.

D. Self-Sovereign Identity

SSI follows a P2P architecture facilitated by blockchain technology, providing global uniqueness, high availability, cryptographic verifiability, and the absence of central authority. Within this architecture, the identity of an individual, group, or connected device is defined by relationships with other peers [25]. These relationships are established through connections, while digital wallets store keys, credentials, and tokens issued by different entities, such as passport offices, driver's license authorities, employers, and loyalty programs.

E. Decentralized Identity Service

Decentralized identity services enable secure and efficient device identity management in distributed environments. The proposed service provides device DID registration and device DID authentication. Device DID registration enables devices to obtain unique decentralized identifiers [26]. Device DID authentication verifies their identities. Together, these functionalities support secure identity management in a decentralized environment.

F. Ai-Integrated Blockchain Iam

- A. The architecture of blockchain-AI integrated cybersecurity systems represents a multi-layered
- B. framework that leverages the strengths of both technologies to deliver intelligent, decentralized, and adaptive
- C. threat mitigation. At its core, such a system typically consists of three primary layers: the data acquisition and
- D. perception layer, the processing and analytics layer powered by AI, and the blockchain-based control and
- E. orchestration layer. These components interact in a looped feedback system that continuously senses, analyzes,
- F. and responds to security events with minimal human intervention (Hassan et al., 2021). The data acquisition and
- G. perception layer gathers information from various endpoints including servers, IoT devices, and user terminals.
- H. This data comprises logs, network traffic, access patterns and sensor readings.
- I. The architecture of blockchain-AI integrated cybersecurity systems represents a multi-layered

- J. framework that leverages the strengths of both technologies to deliver intelligent, decentralized, and adaptive
- K. threat mitigation. At its core, such a system typically consists of three primary layers: the data acquisition and
- L. perception layer, the processing and analytics layer powered by AI, and the blockchain-based control and
- M. orchestration layer. These components interact in a looped feedback system that continuously senses, analyzes,
- N. and responds to security events with minimal human intervention (Hassan et al., 2021). The data acquisition and
- O. perception layer gathers information from various endpoints including servers, IoT devices, and user terminals.
- P. This data comprises logs, network traffic, access patterns and sensor readings.

AI and blockchain integration provides intelligent, decentralized, and adaptive threat mitigation by combining AI-driven analytics with blockchain-based security and access control. The architecture typically consists of three primary layers: the data acquisition and perception layer, the AI-powered processing and analytics layer, and the blockchain-based control and orchestration layer. These layers interact through a continuous feedback system to sense, analyze, and respond to security events with minimal human intervention. The data acquisition and perception layer collects logs, network traffic, access patterns, and sensor readings from endpoints such as servers, IoT devices, and user terminals [27][28].

G. Architecture of Blockchain-Based Identity Management System

The architecture of a blockchain-based identity system is composed of several interacting layers, each performing a specific function to ensure secure, private, and user-controlled identity verification.

- **User Interface Layer:** This layer consists of mobile or desktop applications (digital wallets) that users interact with to manage their DIDs and verifiable credentials [29][30]. Users can present credentials for verification, revoke them, or request new ones [31].
- **Credential Issuance Layer:** Trusted institutions such as universities, government departments, or healthcare providers issue verifiable credentials. These credentials are cryptographically signed and can later be verified by third parties.
- **Verification Layer:** This layer consists of verifiers (like employers or service providers) who validate the credentials using smart contracts and the blockchain [32]. The smart contracts automatically check the issuer's digital signature and credential integrity.
- **Blockchain Layer:** The blockchain functions as the decentralized anchor point. It stores the DIDs,

associated public keys, and registries for revoked credentials. It ensures immutable, timestamped records for public verification.

H. Identity Authentication Based on Blockchain Technology

Currently, there is a significant amount of research on blockchain-based identity authentication. In this section, categorise and introduce these studies from two technical perspectives: identity authentication technologies and encryption algorithms.

- **Password identity authentication:** The most fundamental form of identity authentication, where users verify their identities by inputting pre-set static passwords. However, static password identity authentication has certain security vulnerabilities. For instance, passwords might be maliciously intercepted during transmission or be susceptible to compromise.
- **Public Key Infrastructure (PKI) Identity authentication:** Its identity authentication utilizes asymmetric encryption algorithms to ensure secure identity verification and data transmission [33]. Compared with traditional identity authentication, blockchain-based PKI identity authentication enhances trust among nodes and improves authentication efficiency by leveraging blockchain characteristics.
- **Biometric identity authentication:** A method of identity verification based on individual biological characteristics. It involves generating templates from pre-collected unique biological features of individuals, such as fingerprints, irises, and facial features. During the identity authentication process, the authenticated party's biometric features are compared with previously stored templates to verify identity.

I. Blockchain in Federated Identity Management

The potential application of blockchain technology in the realm of federated identity management (FIM), a system through which users can authenticate across various systems and platforms without establishing a separate identity for each system. The decentralized nature of blockchain was identified as being uniquely applicable to federated identity management, offering a unified and secure way of managing user identities across various platforms [34]. A blockchain-based framework for the purpose of offering a single digital identity for users and hence easy access to various online services. Among the primary advantages highlighted were reducing administrative overhead for identity management across various platforms and offering a more secure and transparent identity authentication process.

J. Challenges of Blockchain-Based Identity Management System

Blockchain-based Identity Management Systems face challenges, which can limit their large-scale deployment. Additionally, issues including high computational overhead, transaction latency, and secure key management must be addressed to ensure efficient, secure, and user-friendly identity management solutions.

- **Regulatory Compliance:** Navigating regulatory compliance in the utilization of blockchain within IAM systems is crucial for ensuring data integrity and protection. As institutions increasingly adopt blockchain paradigms in their IAM frameworks, adherence to regulatory frameworks becomes essential for safeguarding user privacy and ensuring data confidentiality.
- **Evolution of Blockchain Technology:** In the context of modern technological advancement, blockchain technology stands out as a crucial innovation, extending beyond conventional financial transactions. Recent scholarly research highlights its increasing utilization in safety-critical cyber-physical systems, including autonomously navigated vehicles and smart power

distribution networks [35]. This adoption aims to address specific challenges while enhancing operational efficiency.

- **Integration with Emerging Technologies:** The integration of blockchain technology with emerging innovations like machine learning and artificial intelligence holds significant potential to revolutionize IAM systems. Leveraging the capabilities of these cutting-edge technologies, IAM frameworks could enhance security, authentication, and data protection.

Table I summarizes key Blockchain-Based IAM components and their roles in strengthening cybersecurity through secure, transparent, tamper-resistant identity management, access control, authentication, and protection against unauthorized access.

TABLE I. BLOCKCHAIN-BASED IDENTITY AND ACCESS MANAGEMENT FOR CYBERSECURITY

Component	Description	Role in IAM	Cybersecurity Benefits
Blockchain Network	A decentralized ledger that stores identity and access records in an immutable manner.	Maintains secure identity transactions.	Prevents data tampering and provides auditability.
Digital Identity	A unique digital representation of a user, device, or organization.	Identifies entities requesting access.	Reduces identity fraud and impersonation attacks.
Identity Provider (IdP)	Verifies user identities and issues authentication credentials.	Authenticates users before granting access.	Improves trust and secure authentication.
Smart Contracts	Self-executing programs that automatically enforce access policies.	Automates authorization decisions.	Eliminates manual errors and unauthorized access.
Authentication	Process of verifying the identity of a user or device.	Confirms legitimate identities.	Supports multi-factor and decentralized authentication.
Authorization	Determines the permissions assigned to authenticated users.	Controls resource access.	Enforces fine-grained and policy-based access control.
Access Control Policies	Rules defining who can access specific resources.	Manages user permissions.	Ensures least-privilege access and compliance.
User Wallet / Digital Wallet	Stores decentralized identity credentials and cryptographic keys.	Enables secure credential management.	Prevents credential theft through cryptographic protection.
Consensus Mechanism	Validates and confirms blockchain transactions.	Maintains ledger consistency.	Prevents unauthorized modifications and double-spending attacks.
Audit Trail	Immutable record of authentication and authorization events.	Supports monitoring and forensic analysis.	Enhances transparency, accountability, and compliance.

IV. LITERATURE REVIEW

This section highlights related studies on blockchain-based Identity and Access Management (IAM) for cybersecurity, highlighting blockchain, Self-Sovereign Identity (SSI), smart contracts, and AI techniques for secure authentication, authorization, privacy preservation, and decentralized identity management.

G. Maheswari et al. (2026) present a blockchain-based self-sovereign identity framework that achieves these requirements in a way where digital identity management is achieved in a secure environment with decentralization and privacy. That framework also tests the effect of the blockchain consensus

mechanism on the latency of identity verification and discusses blockchain resilience against Sybil attacks and key compromise scenarios. A performance analysis between the two establishes the enhancements in security, transparency, and scalability compared to traditional centralized systems. In order to support its large-scale deployment, the proposed architecture isolates the on-chain metadata from the off-chain credential storage [36].

Rishicharan Reddivari et al. (2025) discuss the structure and features of AI-enabled IAM, such as dynamic authorization, auto identity governance, and context-aware access control. It also discusses the ways that AI systems are learning and adapting based on user behaviour and environmental context to deliver

precise identity verification and granular access decisions. It also touches on deployment considerations like data fidelity, system integration and user buy-in, and highlights strategic benefits including reducing administrative workload, improving compliance, and enabling zero trust security models [37].

R. Raja Sekar et al. (2024) focus on developing a user-centric identity wallet, leveraging blockchain's attributes for transparency, immutability, and cryptographic security, orchestrating smart contracts to automate identity verification and access control. This decentralized IAM architecture not only fortifies security but also empowers users with ownership and sovereignty over their personal data, ensuring a tamper-resistant environment and fostering a more resilient and user-centric digital landscape. The project's strategic alignment with interoperability standards amplifies its impact, promising to set new benchmarks for secure and efficient IAM frameworks across industries [38].

Manasa C. K et al. (2024) propose an innovative approach to optimizing memory utilization for identity management by employing blockchain technology combined with linkable ring signatures. Blockchain delivers a decentralized, immutable, and tamper-proof storage solution, ensuring the integrity and security of digital certificates. Linkable ring signatures provide enhanced privacy and traceability, allowing for anonymous yet verifiable transactions. objective is to create a robust identity management system with superior security and efficacy while

utilizing significantly less RAM by combining these technologies. This method improves identity management system speed across a range of applications in addition minimizing the storage space [39].

S. Pl. Subramaniyan & Sandeep Prabhu (2023) employ a qualitative use case approach to compare traditional identity management with blockchain-based IAM in an enterprise ecosystem. The findings show that blockchain can provide a decentralized and verifiable repository for identity data, enabling legitimate credential verification without disclosing the data itself. Blockchain-based IAM also emphasizes a user-centric approach by giving users control over their digital identities [40].

Taruly Karlina Saragih et al. (2022) present a private blockchain system with Self-Sovereign Identity (SSI) for identity management in the healthcare industry. SSI gives patients control over their medical records with higher security, while healthcare providers benefit from an improved Know Your Customer (KYC) process for new patients. The study suggests several blockchain-based flows to overcome limitations in patient data control and KYC, although implementation requires attention from the surrounding system and stakeholders [41].

Table II compares blockchain-based IAM approaches, highlighting their methodologies, security benefits, limitations, and future directions across enterprise, healthcare, and decentralized identity management environments.

TABLE II. COMPARATIVE ANALYSIS OF BLOCKCHAIN-BASED IDENTITY AND ACCESS MANAGEMENT FOR CYBERSECURITY

Reference	Study Focus	Approach / Methodology	Key Findings	Challenges / Limitations	Future Directions
G. Maheswari et al. (2026)	Blockchain-based SSI Framework	DIDs, VCs, smart contracts, decentralized storage, and blockchain consensus	Provides decentralized, privacy-preserving, tamper-resistant identity management	Verification latency, consensus overhead, deployment complexity	Optimize consensus, scalability, and interoperability
Rishicharan Reddivari et al. (2025)	AI-enabled IAM	ML, behavioural biometrics, predictive analytics, continuous authentication, and adaptive access control	Enables anomaly detection, adaptive authorization, automated governance, and Zero Trust security	Data quality, integration, user adoption, AI reliability	Develop explainable AI and integrate AI with blockchain IAM
R. Raja Sekar et al. (2024)	Blockchain-based User-Centric Identity Wallet	Smart contracts, decentralized wallet, interoperability, and cryptographic security	Enhances identity ownership, secure authentication, and tamper-resistant access control	IAM integration and interoperability challenges	Standardize decentralized identity protocols
Manasa C. K et al. (2024)	Efficient Blockchain Identity Management	Blockchain with Linkable Ring Signatures and optimized memory utilization	Improves privacy, traceability, storage efficiency, and verification	Computational complexity and implementation overhead	Develop lightweight cryptography and scalable storage

S. Subramaniyan & Sandeep Prabhu et al. (2023)	Pl. Blockchain-based IAM for Enterprise Ecosystems	Qualitative use-case comparison of traditional and blockchain IAM	Demonstrates decentralized identity, user control, trust, and secure verification	Limited adoption and organizational trust concerns	Promote enterprise adoption and cybersecurity integration
Taruly Karlina Saragih et al. (2022)	Blockchain-based SSI in Healthcare	Private blockchain for SSI and KYC-based patient identity management	Provides patient-controlled identities, efficient KYC, and improved data security	Stakeholder coordination, integration, and compliance	Improve interoperability and standardized healthcare identity frameworks

V. CONCLUSION AND FUTURE WORK

Blockchain-based Identity and Access Management (IAM) provides a promising approach to addressing the security, privacy, and trust limitations of traditional centralized and federated identity systems. This review examined blockchain architectures, blockchain types, SSI, decentralized identity, smart contracts, blockchain-based authentication, federated identity, and AI-integrated IAM. The reviewed studies demonstrate that blockchain can provide decentralized, tamper-resistant, transparent, and auditable identity management, while SSI improves user ownership and control over digital identities. Smart contracts further support automated authentication and access control, reducing dependence on centralized authorities. The integration of AI strengthens IAM through anomaly detection, behavioural analysis, adaptive authorization, and intelligent threat response. However, challenges including scalability, interoperability, computational overhead, privacy, regulatory compliance, and secure key management remain. Overall, blockchain-based IAM offers a strong foundation for secure, privacy-preserving, user-centric, and resilient cybersecurity environments.

Future research should focus on developing scalable and interoperable blockchain-IAM frameworks that integrate SSI, AI-driven adaptive access control, and privacy-preserving authentication. Lightweight consensus and cryptographic mechanisms can reduce computational overhead and latency. Further work should also address secure key recovery, regulatory compliance, cross-platform interoperability, and real-world enterprise deployment through standardized architectures and extensive performance evaluation.

REFERENCES

1. D. Patel, “Integrating Price Elasticity and Reinforcement Learning: A Data-Driven Framework for Strategic E-commerce Pricing,” in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395747.

2. A. A. Patil, “Research Paper on Cyber Security Challenges and Threats,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 1, pp. 561–566, Jan. 2024, doi: 10.48175/ijarsct-15082.

3. D. N. D. and N. G. Cholli, “A Review on Identity and Access Management Server (KeyCloak),” *Int. J. Secur. Priv. Pervasive Comput.*, vol. 12, no. 3, pp. 46–53, Jul. 2020, doi: 10.4018/ijspcc.2020070104.

4. C. Singh, R. Thakkar, and J. Warraich, “IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations,” *Eur. J. Eng. Technol. Res.*, vol. 8, no. 4, pp. 30–38, Aug. 2023, doi: 10.24018/ejeng.2023.8.4.3074.

5. N. Ghadge, “Use of Blockchain Technology to Strengthen Identity and Access Management (IAM),” 2024. doi: 10.2139/ssrn.4854174.

6. T. Banerjee and H. Singh, “Securing Non-Human Identities in Industrial IoT a Blockchain-Based Trust Framework,” *NIPES - J. Sci. Technol. Res.*, vol. 7, no. 4, pp. 228–246, Dec. 2025, doi: 10.37933/nipes/7.4.2025.1660.

7. A. Goel and Y. Rahulamathavan, “A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility,” *Futur. Internet*, vol. 17, no. 1, p. 1, Dec. 2024, doi: 10.3390/fi17010001.

8. L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems,” Jan. 2020, doi: 10.6028/NIST.CSWP.01142020.

9. Z. Feng, Z. Li, H. Cui, and M. T. Whitty, “Identity Management Systems: A Comprehensive Review,” *Information*, vol. 16, no. 9, p. 778, Sep. 2025, doi: 10.3390/info16090778.

10. T. Surve, A. K. Tyagi, S. Tiwari, and S. Sreevathsa, “Revolutionizing Blockchain Governance: Integrating Gamification, Reputation, and Education into Proxy Voting Systems,” *Procedia Comput. Sci.*, vol. 282, pp. 316–325, 2026, doi: 10.1016/j.procs.2026.05.079.

11. M. M. F. Majeed and A. Adisaputera, “Digital Identity,” *Konfrontasi J. Kult. Ekon. dan Perubahan Sos.*, vol. 7, no. 4, pp. 246–252, Dec. 2020, doi: 10.33258/konfrontasi2.v7i4.122.

12. S. Vitla, “Identity Management in Global Compliance: Innovative Implementation Strategies in Cybersecurity Landscape,” *J. Eng. Res. Reports*, vol. 27, no. 2, pp. 324–340, Feb. 2025, doi: 10.9734/jerr/2025/v27i21412.

13. M. Robles-Carrillo, “Digital identity: an approach to its nature, concept, and functionalities,” *Int. J. Law Inf. Technol.*, vol. 32, no. 1, Jun. 2024, doi: 10.1093/ijlit/eaee019.
14. A. K. Kaleru, “Identity and access management: foundations, principles, and best practices,” *World J. Adv. Eng. Technol. Sci.*, vol. 15, no. 1, pp. 1894–1904, Apr. 2025, doi: 10.30574/wjaets.2025.15.1.0393.
15. M. Epping and M. Morowczynski, “Authentication and Authorization,” *IDPro Body Knowl.*, vol. 1, no. 6, Sep. 2021, doi: 10.55621/idpro.78.
16. A. C. O. Grewe, “An Overview of the Digital Identity Lifecycle (v2),” *IDPro Body Knowl.*, vol. 1, no. 7, Feb. 2022, doi: 10.55621/idpro.31.
17. P. Kilari, “Identity and Access Management in Modern Cybersecurity: Frameworks, Mechanisms, and Strategic Imperatives,” 2023.
18. K. R. Kiran, “API Integration Barriers in Case-Based Process Management: A Review of Interoperability and Real-Time Response Constraints Outline,” *Zenodo*, vol. 25, no. 03, 2025, doi: 10.5281/zenodo.16782616.
19. V. H. S. Quraishi, “A Review on Blockchain-Based Identity Management System,” in *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, IEEE, Apr. 2022, pp. 735–740. doi: 10.1109/ICIEM54221.2022.9853110.
20. S. Singh, “Advancing Wireless Communications with Open Radio Access Network,” in *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, IEEE, Jul. 2025, pp. 682–687. doi: 10.1109/ICDICI66477.2025.11135206.
21. M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, “Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey,” *IEEE Access*, vol. 10, pp. 113436–113481, 2022, doi: 10.1109/ACCESS.2022.3216643.
22. N. Sethi, “Blockchain Architecture and Consensus Mechanisms: Challenges, Innovations, and Future Trends,” *Int. J. Comput. Appl.*, vol. ICAIDSC202, no. 3, pp. 28–35, Jan. 2025, doi: 10.5120/icaidsc202423.
23. P. Maidamwar and N. Chavhan, “Blockchain Technology: A Review on Architecture, Security Issues and Challenges,” *Int. J. Eng. Appl. Sci. Technol.*, vol. 04, no. 12, pp. 245–249, May 2020, doi: 10.33564/IJEAST.2020.v04i12.039.
24. Y. Muni, “A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks,” *Eng. Technol. J.*, vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.21.
25. D. C. N. Kyriakidou, A. M. Papathanasiou, and G. C. Polyzos, “Decentralized Identity With Applications to Security and Privacy for the Internet of Things,” *Comput. Networks Commun.*, Aug. 2023, doi: 10.37256/cnc.1220233048.
26. B. Zaghdoudi, G. Bu, M. Potop-Butucaru, and S. Fdida, “Blockchain-Based Decentralized Identity System: Design and Security Analysis,” in *2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, IEEE, Jun. 2025, pp. 261–265. doi: 10.1109/DCOSS-IoT65416.2025.00044.
27. O. Charles and C. O. Nwankwo, “Blockchain and Artificial Intelligence Integration in Cybersecurity: Towards Intelligent and Decentralized Defenses,” 2025.
28. Y. Muni, “Advanced Multi-Protocol Label Switching (MPLS)-Enabled Networks: A Survey of Emerging Approaches Via Traffic Engineering,” *Eng. Technol. J.*, vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.22.
29. R. Lingam, “AI-Powered Framework for Evaluating Child-Friendly Mobile Applications,” *Int. J. Hum. Comput. Intell.*, vol. 4, no. 4, pp. 535–549, 2025, doi: 10.5281/zenodo.15624307.
30. R. Palwe, “Three Layers of Trust in AI Interfaces: Interface, Behaviour, and Organization,” *Int. J. Sci. Res.*, vol. 15, no. 1, pp. 1152–1160, Jan. 2026, doi: 10.21275/SR26112072531.
31. R. K. Kanneganti, “Impact of Custom Interface Widgets on User Efficiency in Content Navigation Platforms,” *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 1, no. 01, pp. 179–186, Aug. 2023, doi: 10.58812/esiscs.v1i01.1121.
32. R. Narayanan, S. Agarwal, and N. Pal, “Blockchain-Based Identity Management Systems: Ensuring Privacy and Data Integrity through Decentralized Verification,” vol. 10, no. 1, pp. 27–40, 2025.
33. J. Li, “A review of identity authentication based on blockchain technology,” *Appl. Comput. Eng.*, vol. 30, no. 1, pp. 173–178, Jan. 2024, doi: 10.54254/2755-2721/30/20230094.
34. S. Tiwari and R. Agarwal, “Blockchain-Driven IAM Solutions: Transforming Identity Management in the Digital Age,” 2025. doi: 10.2139/ssrn.5259377.
35. N. Ghadge, “Analyzing the Role of Blockchain in Identity and Access Management Systems,” *Int. J. Sci. Res. Arch.*, vol. 12, no. 1, pp. 2249–2256, Jun. 2024, doi: 10.30574/ijrsra.2024.12.1.1019.
36. G. Maheswari, G. S. Koushik Reddy, J. Nikhil Naik, G. K. Sree, and C. Anitha, “A Blockchain-based Self-Sovereign Identity Framework for Secure and Privacy-Preserving Digital Identity Management,” in *Proceedings of 6th International Conference on Expert Clouds and Applications, ICOECA 2026*, IEEE, Mar. 2026, pp. 1393–1398.

- doi: 10.1109/ICOECA68095.2026.11485511.
37. R. Reddivari, B. B. Chavan, and B. Pandey, “AI-Integrated Identity and Access Management: Advancing Cybersecurity through Intelligent Access Control and Continuous Authentication,” in *2025 IEEE Madhya Pradesh Section Conference (MPCON)*, IEEE, Aug. 2025, pp. 505–511. doi: 10.1109/MPCON66082.2025.11256518.
38. R. R. Sekar, A. Masna, S. Sharma, A. Abraham, and P. R. Pagilla, “Decentralized Identity and Access Management (IAM) Using Blockchain,” in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, IEEE, May 2024, pp. 1–6. doi: 10.1109/ISCS61804.2024.10581159.
39. M. C. K, U. M, V. E. V, G. G, S. R, and S. C. K, “Efficient Certificate Storage and Compression: Optimizing Memory Utilization for Identity Management Using blockchain,” in *2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N)*, IEEE, Dec. 2024, pp. 1780–1784. doi: 10.1109/ICAC2N63387.2024.10894951.
40. S. P. Subramaniyan and S. Prabhu, “The Impact of Adopting Blockchain-based Identity Access Management: Current Applications and Potential Directions,” in *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, IEEE, May 2023, pp. 1240–1245. doi: 10.1109/ICAAIC56838.2023.10140585.
41. T. K. Saragih, E. Tanuwijaya, and G. Wang, “The Use of Blockchain for Digital Identity Management in Healthcare,” in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*, IEEE, Sep. 2022, pp. 1–6. doi: 10.1109/CITSM56380.2022.9935935.