ISSN: 2959-6386 (Online), Vol. 2, Issue 2

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

JKLST
ISSN 2959-6386
VOLUME 2 ISSUE 2
EXPLORING THE INTERSECTION OF
KNOWLEDGE, LEARNING, AND SCIENCE & TECHNOLOGY:
UNLEASHING THE POWER OF SYNERGY
IN THE 21ST CENTURY

Privacy-Preserving AI/ML Application Architectures: Techniques, Trade-offs, and Case Studies

Lavanya Shanmugam[1], Ravish Tillu[2], Suhas Jangoan[3]

[1]Tata Consultancy Services, USA
[2]RBC Capital Markets, USA
[3]Zendesk, USA

Abstract

Given the widespread adoption and fusion of artificial intelligence (AI) and blockchain technologies, safeguarding privacy has become paramount. These techniques not only ensure the confidentiality of individuals' data but also uphold the integrity and reliability of the information. This study provides an introductory overview of AI and blockchain, elucidating their fusion and subsequent emergence of privacy protection methodologies. It delves into specific application contexts such as data encryption, de-identification, multi-tier distributed ledgers, and k-anonymity techniques. Furthermore, the paper critically assesses five pivotal dimensions of privacy protection systems within AI-blockchain integration: authorization management, access control, data security, network integrity, and scalability. Additionally, it conducts a thorough analysis of existing shortcomings, pinpointing their root causes and proposing corresponding remedies. The study also categorizes and synthesizes privacy protection methodologies based on AI-blockchain application contexts and technical frameworks. In conclusion, it outlines prospective avenues for the evolution of privacy protection technologies stemming from the integration of AI and blockchain, emphasizing the need to enhance efficiency and security for a more holistic safeguarding of privacy.

Keywords: Artificial Intelligence; Blockchain Privacy Protection; Data Encryption; De-identification; Access Control

Article Information:
Article history: *Received:* 01/11/2023 *Accepted:* 10/11/2023 *Online:* 16/11/2023 *Published*: 16/11/2023
DOI: https://doi.org/10.60087/jklst.vol2.n2.p420

Correspondence Author: Lavanya Shanmugam

Introduction

In recent years, the integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies has revolutionized numerous industries, driving innovation and efficiency. However, with the increasing reliance on AI/ML applications, concerns regarding data privacy and security have become paramount. As organizations collect vast amounts of sensitive data for training and deploying AI models, ensuring privacy protection has emerged as a critical challenge.

To address these concerns, privacy-preserving AI/ML application architectures have gained significant attention. These architectures aim to implement robust techniques and strategies to safeguard sensitive data while harnessing the power of AI and ML for insights and decision-making. In this context, understanding the various techniques, trade-offs, and real-world case studies becomes essential for organizations seeking to adopt privacy-preserving AI/ML solutions.

This paper delves into the intricate landscape of privacy-preserving AI/ML application architectures. It explores a diverse range of techniques employed to protect data privacy while maintaining the efficacy of AI/ML models. From encryption methods to differential privacy frameworks, each technique comes with its unique trade-offs, balancing privacy requirements with performance and usability considerations.

Furthermore, the paper examines real-world case studies across different industries, showcasing how organizations have successfully implemented privacy-preserving AI/ML application architectures to address specific challenges. These case studies provide valuable insights into the practical implications, challenges faced, and lessons learned in deploying privacy-preserving AI/ML solutions.

By synthesizing the latest research findings, industry practices, and practical experiences, this paper aims to offer a comprehensive overview of privacy-preserving AI/ML application architectures. It equips readers with the knowledge and insights needed to navigate the complex landscape of privacy protection in AI/ML applications, empowering organizations to make informed decisions and develop robust privacy-preserving strategies for their AI initiatives.

Privacy Security in AI and Blockchain

1. Development of Blockchain Technology

The advent of the Bitcoin blockchain system, introduced by Nakamoto in November 2008 [1], has sparked global interest and extensive discussions. The meteoric rise in Bitcoin's value has popularized the term "cryptocurrency" in both industrial and academic circles. As of February 18, 2023 [2], Bitcoin's circulating market capitalization reached RMB 3.25 trillion, underscoring its significant commercial value and the immense potential of virtual currencies in the financial landscape. This surge in value has also reignited research and development efforts in blockchain technology. The initial phase, known as Blockchain 1.0, primarily leverages distributed ledgers. The advent of Ethereum in 2014 marked a pivotal moment in the era of Blockchain 2.0, integrating innovative technologies like smart contracts [3]. Blockchain 3.0 has ushered in application platforms for the Internet of Things and smart healthcare [4], while Blockchain 4.0 is poised to create a robust ecosystem and expand blockchain technology's applications across various sectors, including cultural and entertainment, and communication infrastructure [5].

Blockchains are categorized based on their accessibility and control levels, primarily as public, private, and federated chains. Public blockchains like Bitcoin and Ethereum boast decentralization, allowing nodes to join or exit the network freely, fostering maximum decentralization. Federated chains, exemplified by FISCO BCOS [6], enable smart contract implementation using Turing-complete language and employ homomorphic cryptography for privacy protection, albeit with partial decentralization. Conversely, private blockchain networks such as Antchain regulate node permissions while offering faster transaction processing and lower fees.

The Ethereum blockchain's structure, illustrated in Figure 1, employs a linked list data structure to interconnect multiple blocks [7]. Each block header stores the hash address of the preceding block, ensuring a sequential linkage between successive blocks. Despite the myriad benefits of blockchain technology, security concerns across various domains cannot be overlooked. In the financial sector, the economic ramifications of privacy breaches are immeasurable [8]. Protecting user assets and identity information has become paramount in blockchain security research, given their critical nature and the potential threat posed by malicious nodes. Security remains an indispensable aspect of any industry or technology, with blockchain security being vital for its sustainable development.

Ethereum operates as a decentralized blockchain platform, where multiple nodes collaboratively maintain a shared ledger of information. Each node utilizes the Ethereum Virtual Machine (EVM) to execute smart contracts, communicating via a peer-to-peer network [9]. Nodes are endowed with distinct functions and permissions, yet all can collect transactions and participate in block mining. Upon acquiring bookkeeping authority, an Ethereum node publishes a block, with other nodes ensuring data consistency through the Proof of Stake (PoS) consensus mechanism.

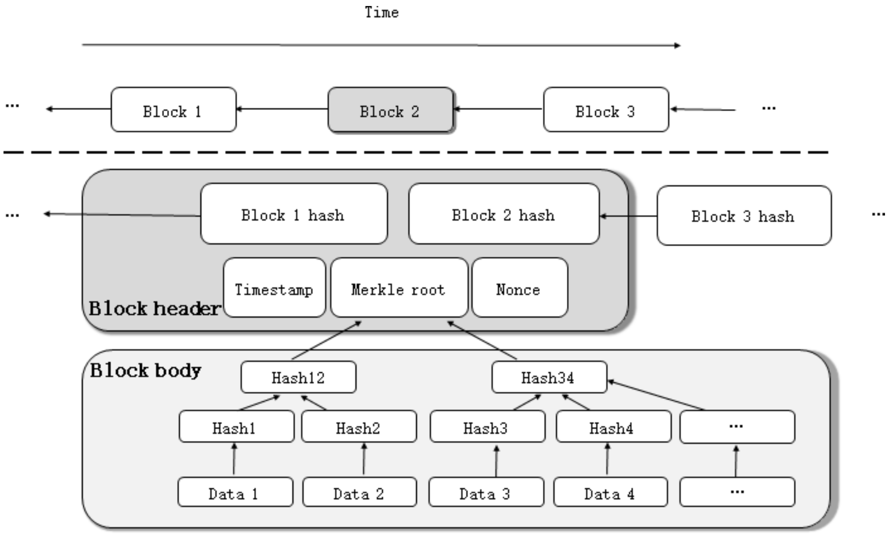


Figure 1: Structure of the Ethereum Blockchain

The Ethereum blockchain structure is characterized by its rapid block generation speed, approximately 15 seconds per block, surpassing Bitcoin in this aspect. This feature enables miners to receive block rewards at a faster rate and significantly reduces the time required for transaction verification. Additionally, Ethereum facilitates the implementation of smart contracts, enabling users to develop various applications such as digital wallets and decentralized applications (DApps).

2. Artificial Intelligence

Artificial intelligence (AI) [10] is a discipline focused on developing computer systems capable of emulating autonomous thinking and decision-making processes. The goal of AI is to make informed judgments and efficiently execute predefined tasks. Recent groundbreaking achievements, such as DeepMind's AlphaGo becoming the world champion and the success of OpenAI's ChatGPT model, have propelled AI into the spotlight, garnering significant interest worldwide. Subfields of AI include deep learning, natural language processing (NLP), and others, all interconnected by their fundamental objective of analyzing and interpreting data.

Natural Language Processing (NLP) [10] is a critical subfield of AI that deals with processing various types of text and linguistic data. Advances in deep learning have led to the development of top-tier NLP models such as BERT and GPT. NLP utilizes specialized processing techniques or models to analyze data computationally, enabling tasks like text categorization, speech recognition, and machine translation.

The initial step in NLP involves transforming text into a format understandable by computers. However, this task is complicated by language complexity, ambiguity, and the need for precise evaluation criteria. Researchers address these challenges by employing specific symbolic representations and neural network architectures tailored to different NLP tasks.

Deep Learning (DL) [12] is a cornerstone of AI, modeled after the structure of neurons in the human brain. DL processes input information through hierarchical network structures, layer by layer, to generate a final representation. DL encompasses supervised and unsupervised learning methods and has significantly influenced fields such as image processing, speech recognition, and NLP.

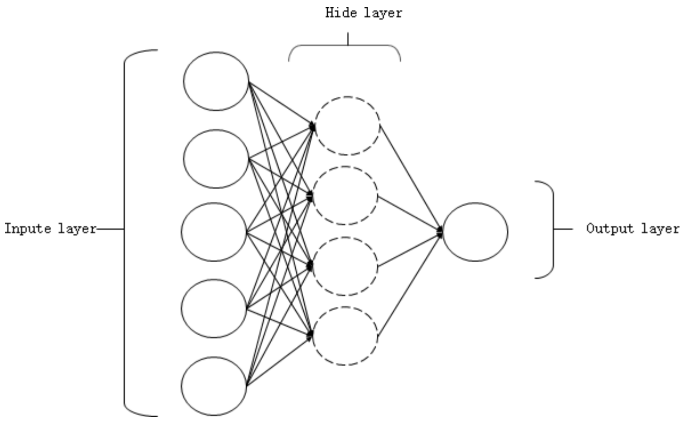


Figure 2: Deep Learning Perceptron Architecture

In Figure 2, deep learning (DL) utilizes a multi-level neural network architecture to extract data features. This neural network comprises three main types of layers: the input layer, the hidden layer, and the output layer. Each layer of perceptrons is interconnected, forming the deep learning model. With the advent of distributed deep learning, computational parameters such as eigenvalues and gradient values become vital information transmitted between nodes during model training. However, the presence of malicious nodes poses a threat as they could intercept computation results using sophisticated attack algorithms, potentially resulting in the exposure of sensitive data through reverse inference or data leakage.

3. Convergence of Artificial Intelligence and Blockchain Technologies

In today's information age, the integration of artificial intelligence (AI) and blockchain technologies is becoming increasingly prevalent across diverse domains, highlighting the significance of addressing data security and privacy concerns. Innovative initiatives such as Anthropic’s Constitutional AI [13], SingularityNET’s Decentralized AI [14], and ChainLink’s Decentralized Oracle [15] epitomize the deep integration of AI and blockchain technologies, aiming for more efficient, secure, and transparent data processing.

Anthropic’s Constitutional AI system leverages large-scale models and blockchain technologies to uphold audit tracking and accountability throughout the model training process, encompassing data, parameters, and outputs. Similarly, SingularityNET’s Decentralized AI system deploys AI models on blockchain networks, fostering decentralized collaboration and services among models. This setup enables users to conveniently access models, adjust parameters, and access highly reliable services. Furthermore, ChainLink's Decentralized Oracle system enables blockchain networks to securely interact with off-chain AI models and datasets while verifying inputs and outputs, thereby providing a trustworthy external information source for blockchains.

These integrated systems exhibit the convergence of artificial intelligence and blockchain technologies through the following aspects:

1. Utilization of blockchain technology to store and record model parameters, training data, and inputs and outputs, ensuring transparency in model audits and fostering accountability.
2. Deployment of AI models on blockchain networks to facilitate decentralized collaboration and services among models, thereby enhancing system stability and scalability.
3. Facilitation of secure access to external AI models and data through decentralized systems, empowering blockchain networks to acquire reliable external information.
4. Harnessing blockchain-based incentive mechanisms and token designs to establish motivating connections and trust interactions between AI model developers and users.

Blockchain Privacy Protection

Blockchain technology, characterized by its distributed ledger system and consensus algorithms like Proof of Stake (PoS) [16], ensures on-chain data integrity and transaction encryption through cryptographic methods. However, despite its transparency, the exposure of sensitive data on the blockchain poses challenges to data privacy and security [17], particularly in use cases such as financial applications and supply chain management, where transaction data confidentiality is crucial. To address these challenges and broaden the scope of blockchain applications, ensuring data security and privacy protection becomes imperative.

Several data protection technologies have been proposed to enhance data privacy on the blockchain, including zero-knowledge proof, ring signatures, homomorphic encryption, and secure multi-party computation [18]. Each of these technologies offers unique capabilities in safeguarding data privacy:

Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) is a cryptographic technique introduced by Goldwasser et al. [19] in 1985. It enables a prover to demonstrate the correctness of a statement to a verifier without revealing any information beyond the validity of the statement. In the blockchain context, ZKP protocols like zk-SNARKs are commonly used to achieve privacy by generating succinct proofs without disclosing underlying data, enabling functionalities like decentralized coin-mixing pools for enhanced privacy [20].

Ring Signature

Ring Signature (RS), proposed by Rivest in 2001 [21], allows a signer to hide their identity among a group of users, forming a ring of equal-status participants. Applied to the blockchain, RS conceals transaction addresses, making it difficult for attackers to infer traders' identities. By choosing members within the ring, users enhance privacy, with variations such as threshold ring signatures offering additional flexibility and security.

Homomorphic Encryption (HE)

Homomorphic Encryption (HE) is a cryptographic technique integral to blockchain development. HE allows operations on encrypted data without revealing plaintext, offering both confidentiality and data availability. With partial and fully homomorphic encryption, users can perform computations on encrypted data securely, ensuring privacy while maintaining computational efficiency [22].

Each of these privacy protection technologies contributes to enhancing data privacy on the blockchain, addressing concerns related to confidentiality and security.

Artificial Intelligence Privacy Protection Technology

In the era of advanced AI technologies, ensuring the privacy of sensitive personal data is paramount, particularly in domains like healthcare and finance. With AI models continually evolving, including language analysis and perception models like ChatGPT, maintaining privacy while utilizing sensitive data becomes crucial. Various privacy protection techniques, such as secure multi-party computation and homomorphic encryption, play essential roles in safeguarding sensitive information across diverse AI applications.

Secure Multi-party Computation (SMPC)

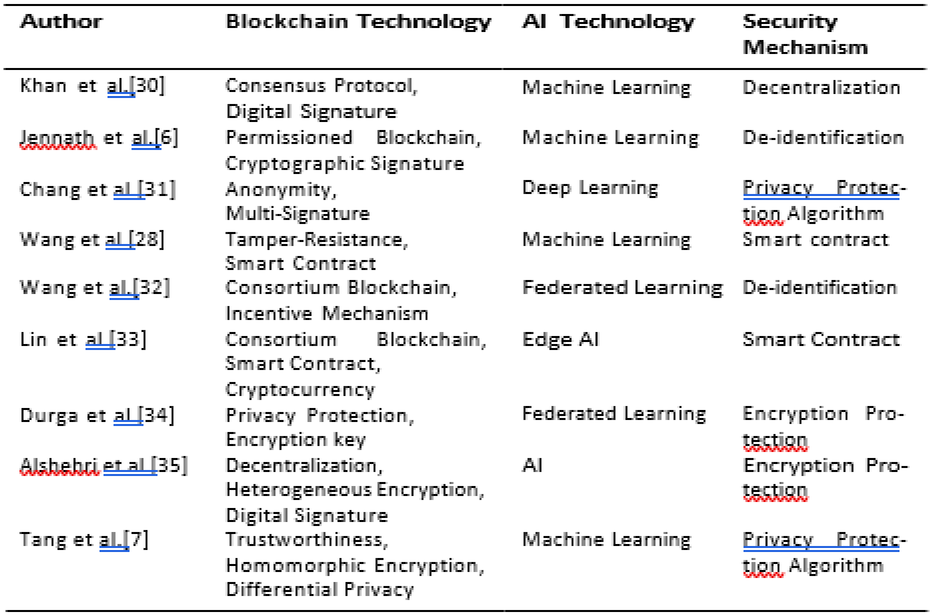
Secure Multi-party Computation (SMPC) allows multiple participants to collaboratively process private data without revealing individual inputs. Protocols like garbled circuits and secret sharing enable secure computation of functions while preserving data privacy, ensuring that each participant only accesses their computed values [24].

Differential Privacy

Differential privacy, proposed by Dwork et al. in 2006 [26], focuses on preserving data privacy by adding controlled noise to sensitive information during data processing. By balancing data distortion and privacy requirements, differential privacy techniques ensure that sensitive information does not unduly influence data queries, thereby mitigating privacy risks while maintaining data utility [27].

Overall, advancements in privacy protection technologies enable the responsible and secure utilization of sensitive data in AI applications, addressing concerns related to privacy infringement and data misuse.

Table 1: Summary of the Applications of Blockchain in AI Privacy Protection



Author	Blockchain Technology	AI Technology	Security Mechanism
Khan et al.[30]	Consensus Protocol, Digital Signature	Machine Learning	Decentralization
Jennath et al.[6]	Permissioned Blockchain, Cryptographic Signature	Machine Learning	De-identification
Chang et al.[31]	Anonymity, Multi-Signature	Deep Learning	Privacy Protection Algorithm
Wang et al.[28]	Tamper-Resistance, Smart Contract	Machine Learning	Smart contract
Wang et al.[32]	Consortium Blockchain, Incentive Mechanism	Federated Learning	De-identification
Lin et al.[33]	Consortium Blockchain, Smart Contract, Cryptocurrency	Edge AI	Smart Contract
Durga et al.[34]	Privacy Protection, Encryption key	Federated Learning	Encryption Protection
Alshehri et al.[35]	Decentralization, Heterogeneous Encryption, Digital Signature	AI	Encryption Protection
Tang et al.[7]	Trustworthiness, Homomorphic Encryption, Differential Privacy	Machine Learning	Privacy Protection Algorithm

Privacy Protection Through the Integration of AI and Blockchain Technologies

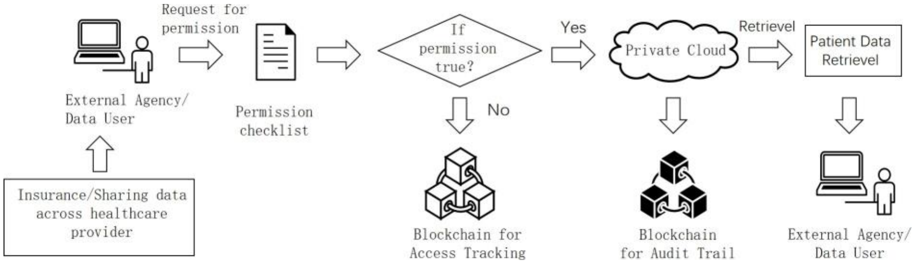

Request for permission
External Agency/ Data User
Insurance/Sharing data across healthcare provider
Permission checklist
If permission true?
Yes
No
Blockchain for Access Tracking
Private Cloud
Retrievel
Blockchain for Audit Trail
Patient Data Retrievel
External Agency/ Data User

Figure 3: Patient Data Request Process

Currently, the reliability of data transmission within the data trust system faces limitations [28], jeopardizing data security and privacy. To tackle this challenge, integrating blockchain technology can establish a robust and trustworthy data storage and sharing system, bolstering data security and privacy protection [29]. Table 1 outlines specific applications of integrating artificial intelligence and blockchain in privacy protection technology. Strengthening the integration and deployment of these technologies can significantly enhance the security and protective capabilities of the existing data trust system.

Data Encryption

Conventional data storage and sharing methods are susceptible to various security threats [30][6][31], particularly due to their reliance on centralized servers, making them easy targets for attackers and resulting in issues like data leaks and tampering. Traditional encryption methods are no longer adequate to address the growing security needs [34][35].

To combat these challenges, privacy protection technology combining artificial intelligence and blockchain has emerged. Leveraging distributed encryption algorithms significantly elevates the security and privacy protection level of data.

Given that traffic and vehicle data often contain sensitive personal information, Wang et al. [32] introduced a blockchain-based privacy-preserving federated learning (FL) scheme. This scheme enhances the Multi-Krum technique by integrating it with homomorphic encryption to achieve ciphertext-level model aggregation and filtering, enabling verification of local models while ensuring privacy protection. In this scheme, the Paillier homomorphic encryption technique [36] encrypts model updates, providing additional privacy protection.

The Paillier algorithm operates as follows:

(1) Key generation: Selecting two random large prime numbers p and q such that n_0 and λ satisfy Formula 2 and Formula 3, respectively. Then, choose a value g from set B that satisfies Formula 5 based on Formula 4.

$$\text{Paillier.Genkey()} \rightarrow (n_0, g), (\lambda, \mu)$$

$$n_0 = p \times q$$

$$\lambda = \text{lcm}(p - 1, q - 1)$$

\[L(x) = \frac{{x - 1}}{{n_0}} \]

\[\gcd(L(g^{\lambda \bmod n^2})) \]

(2) Encryption: Apply the Paillier algorithm using Formula 6.

\[\text{Paillier.Enc(m)} \rightarrow c = g^m \cdot r^{n_0} \bmod n^2 \]

(3) Decryption: Decrypt the ciphertext \(c \) using Formula 7, where \(m < n_0 \).

\[\text{Paillier.Dec(c)} \rightarrow m = \frac{{L(c^{\lambda \bmod n^2})}}{{L(g^{\lambda \bmod n^2})}} \bmod n_0 \]

Here, \((n_0, g) \) represents the public key, while \((\lambda, \mu) \) denotes the private key. \(m \) represents the plaintext, \(r < n_0 \) is a random number.

De-identification

De-identification is a widely used technique for anonymizing personal identification information in data by separating data identifiers from the data itself, thereby mitigating data tracking risks. Jennath et al. [7] proposed a decentralized artificial intelligence framework based on permissioned blockchain technology that employs this approach. The framework effectively segregates personal identification information from non-personal identification information and stores the hash value of personal identification information in the blockchain. This approach enables sharing of medical data without disclosing patient identities. The framework utilizes two independent blockchains for data requests, as illustrated in Figure 3. One blockchain stores patient information and data access permissions, while the other logs audit traces of queries or requests made by requesters. This design empowers patients with full ownership and control over their data while facilitating secure data sharing among multiple entities.

Multi-layered Distributed Ledger

A multi-layer distributed ledger is a decentralized data storage system comprising multiple hierarchical layers designed to facilitate efficient and secure data sharing while ensuring privacy protection [31][7].

Chang et al. [31] introduced DeepLinQ, a blockchain-based multi-layer distributed ledger aimed at addressing users' privacy concerns related to data sharing by enabling privacy-protected data sharing. DeepLinQ leverages blockchain features such as complete decentralization, consensus mechanisms, and anonymity to safeguard data privacy. It achieves this through various techniques including on-demand querying, proxy reservation, subgroup signatures, access control, and smart contracts. By employing these techniques, DeepLinQ enables privacy-protected distributed data sharing.

K-anonymity

The K-anonymity method [37][38] is a privacy protection technique that focuses on grouping individuals in a dataset in a manner where each group comprises at least K individuals with identical attribute values, thereby safeguarding individual privacy.

Long et al. [37] proposed a robust transactional model based on the K-anonymity method for transactions between electric vehicles and energy nodes. In this model, the K-anonymity method serves two primary purposes: firstly, to conceal user identifiers to prevent attackers from linking users to their electric vehicles, and secondly, to obfuscate the location of electric vehicles by constructing a unified request using K-anonymity techniques to conceal the car owner's location.

Evaluation and Situation Analysis

Authority Management

Access control serves as a critical security measure, regulating user access to authorized resources based on predefined rules or policies to uphold system security and data integrity. Consequently, designing and implementing access control is of paramount importance in the realm of blockchain and AI systems.

TURKI et al. [41] pioneered an intelligent privacy parking management system leveraging AI and blockchain technology, employing a Role-Based Access Control (RBAC) model for permission management [42, 43, 44, 50, 51, 52]. Within this model, users are assigned distinct roles and categorized accordingly to govern attribute access permissions. Participants utilize their blockchain addresses to verify their identities and execute attribute authorization access.

Similarly, Ali et al. [49] crafted a privacy protection and intrusion detection framework grounded in blockchain and deep learning, delineating four distinct levels of access control policies. The framework encompasses Membership Service Participants (MSPs) entrusted with managing client registration and authentication processes, alongside the issuance and storage of participant certificates. Additionally, Key Verifiers (KVs) are tasked with verifying user identities and certificates upon request.

Access Control

Access control stands as a pivotal mechanism for ensuring privacy protection, regulating access based on user identity and group membership to guarantee that only authorized users can reach specific resources, thus shielding the system from unauthorized intrusion. To attain effective access control, various factors such as user authentication [41], authorization [48], and access policies [42] must be meticulously considered and implemented. Only through the meticulous integration of these aspects can privacy and security be upheld within the system.

Digital Identity Technology (DIT) [40, 41, 42, 48, 53] emerges as a promising approach for IoT applications, furnishing secure access control and safeguarding device and data privacy. Wazid et al. [47] proposed a suite of access control policies rooted in digital identity technology and cryptographic primitives to fortify communication security among entities like drones, Ground Station Servers (GSS), and cloud servers. Upon the entity's registration in the trusted control room, credentials are securely stored in memory and mobile devices. Following user authentication and key establishment, the user dispatches a request to the GSS using a session key, prompting the GSS to issue an encrypted command message with the current timestamp to the drone. Subsequently, the drone verifies its identity with the GSS and establishes a secure communication key between them.

Lee et al. [48] introduced blockchain-based access tokens to authenticate access control policies inscribed in smart contracts, deploying these access tokens to authenticate Docker Registry, thereby ensuring that solely authorized users can access the encapsulated models. These technologies proffer efficient and dependable secure access control mechanisms in IoT environments.

Despite advancements, some systems still falter in implementing effective access control. Table 4 encapsulates the types of deficiencies and the implicated layers. Potential reasons include:

1. Unreasonable system design: The system design process may inadequately consider privacy protection and access control or overlook the necessity for robust identity authentication and access control based on the system's usage scenarios and requirements.
2. Inadequate permission control: Insufficient granularity in access control results in users acquiring unnecessary permissions, spawning security vulnerabilities.

Absence or inadequacy in access control mechanisms during the design and development phases of privacy protection systems integrating artificial intelligence and blockchain exposes them to security risks and privacy breaches, jeopardizing system stability and integrity.

Data Protection

Data protection encompasses various measures such as access control, data encryption [40, 54], data backup, and security auditing, all aimed at preventing illegal access, tampering, or leakage of user data. In terms of data processing, technologies like anonymization [42], data masking [46], data encryption, and data isolation [55] serve to shield data from unauthorized access and leakage. Additionally, encryption technologies such as differential privacy protection [45], homomorphic encryption [49], hash algorithms [42, 47], digital signature algorithms [49], and asymmetric encryption algorithms [46, 48] play crucial roles in ensuring data confidentiality and preventing unauthorized access by non-authorized users.

Wan et al. [45] employed homomorphic encryption to encrypt the local model parameters of edge devices before uploading them to the central server. The central server then aggregates ciphertext parameters from all clients and sends the updated global model back to each client for decryption, completing the training process. Furthermore, this study integrated differential privacy protection to safeguard the privacy of local model parameters by introducing noise data, such as Laplace noise [56], to the response, thus preventing privacy data leakage.

Lee et al. [48] introduced a management framework leveraging blockchain and AI technology to safeguard the privacy of digital assets. This framework utilizes OrbitDB as an off-chain distributed database to store the personal data of end-users. Prior to service provision, permission to access the personal OrbitDB database of the end-user is required. The end-user utilizes asymmetric encryption algorithms to encrypt the OrbitDB address with the public key PKenc and encrypts the data stored in OrbitDB with the public key PKdata, ensuring that the data remains unreadable in plaintext. This approach ensures data security and privacy, preventing data abuse.

Despite the widespread use of encryption technology for data security, it serves only as a partial safeguard for data protection. Therefore, adopting multiple security technologies is imperative to establish a comprehensive security system ensuring data security. As summarized in Table 5, issues related to data protection in the system often stem from:

1. Heavy reliance on blockchain for security, neglecting other cryptographic measures during the design phase.
2. Difficulties in designing encryption algorithms based on real-world scenarios, necessitating a deep understanding of cryptographic algorithms and practical scenario demands.

Careful consideration during system design and continuous attention to the development of cryptographic algorithms and cryptographic technology are essential. The adoption of a combination of multiple technologies is vital to ensure the confidentiality, integrity, and reliability of data and to protect user privacy.

3.4. Network Security

Network security encompasses various aspects such as preventing network attacks, ensuring data confidentiality and integrity, and safeguarding systems from malicious software and network viruses. To achieve system security and reliability, a series of security measures, secure network architectures, and protocols need to be implemented [57]. Additionally, assessing and analyzing different network threats and developing corresponding security strategies and defense mechanisms are essential to enhance the security and reliability of the system.

Ali et al. [49] proposed a privacy-preserving and intrusion detection framework based on blockchain and deep learning. This framework incorporates an Intrusion Detection System (IDS) that monitors and analyzes network traffic. The IDS identifies intrusions using feature-based and anomaly-based methods. The former matches rules/signatures with a database of known rules, while the latter relies on interpreting normal activity to identify deviations. Deep learning algorithms automatically reduce the complexity of network traffic to identify correlations between data, effectively detecting intrusion behavior.

Singh et al. [40] introduced an IoT healthcare privacy protection framework that integrates federated learning and blockchain technology. This framework enhances security by introducing protocols in IoT devices and intelligent systems. These protocols facilitate the exchange of initial control messages to ensure features such as message authentication, complete forward secrecy, and prevention of replay attacks, thereby thwarting attempts by eavesdroppers to invade patient privacy.

The types and features of network attacks that may target privacy protection systems based on the integration of artificial intelligence and blockchain. For systems lacking effective network security measures, Table 6 outlines relevant design characteristics and system-level measures to prevent scenarios such as over-reliance on the security of the blockchain network, neglecting the design and implementation of security protocols, and prioritizing functionality and performance at the expense of security.

The absence of network security protection in a system may lead to various security threats and risks, potentially resulting in leakage and misuse of sensitive data and privacy information, causing significant losses to individuals and businesses. Therefore, ensuring network security protection is crucial in privacy protection systems based on the integration of artificial intelligence and blockchain.

Scalability

Scalability refers to a system's ability to accommodate a growing number of users or larger volumes of data. When designing for scalability, factors such as system performance, node management, data storage, and transmission must be carefully considered. It's essential to ensure that system scalability is achieved without compromising security, thus preventing security risks and data breaches.

Lee et al. [48] devised a system complying with the European General Data Protection Rules (GDPR) by storing artwork metadata and privacy-related data in a distributed file system off the chain. Digital tokens and artwork metadata are stored in OrbitDB, a database distributed across multiple nodes to ensure data security. This off-chain distributed approach enhances system scalability by dispersing data storage.

Wan et al. [45] introduced a blockchain-based B5G edge device privacy protection framework utilizing federated learning to achieve distributed learning of local data. The central server aggregates encrypted local parameters from all clients and updates the global model. Employing blockchain technology decentralizes the federated learning server, reducing single-point failure risks and poisoning attacks. Additionally, this framework's versatility allows for application across various datasets, models, computing resources, and algorithms, enhancing system scalability. Furthermore, it improves model interpretability and effectively manages bias and noise.

This study identifies that many systems lack adequate scalability design or excessively rely on blockchain's distributed nature. Blockchain faces scalability challenges such as scaling issues, low transaction processing speeds, and interoperability problems. Table 7 outlines the challenges and difficulties encountered when designing systems with robust scalability.

To enhance system scalability, techniques like distributed storage, distributed computing, data sharding, and parallel processing can be employed. In privacy protection systems integrating artificial intelligence and blockchain, scalability is particularly crucial due to processing extensive volumes of sensitive data. Thus, scalability considerations are imperative to ensure continuous and stable system operation. Technologies such as InterPlanetary File System (IPFS) [48, 58], federated learning [40, 42, 59, 60], data sharding, and parallel computing [62] can all contribute to improving system scalability.

Situation Analysis

The fusion of blockchain technology and AI has led to the development of a system effectively safeguarding user privacy data. While challenges persist, including data protection, access control, network security, and scalability, it's essential to comprehensively address these issues during the design phase based on practical considerations. As technology evolves and application scenarios expand, this privacy protection system based on blockchain and AI is expected to garner significant attention and research in the future.

Based on research findings, application scenarios, and technical approaches, we can categorize them into three main groups:

1. Privacy protection applications in the Internet of Things (IoT) leveraging both artificial intelligence and blockchain technology.
2. Privacy protection applications in smart contracts and services integrating artificial intelligence and blockchain technology.
3. Large-scale data analysis techniques utilizing artificial intelligence and blockchain technology for privacy protection.

Each category focuses on distinct aspects of privacy protection, leveraging the combined strengths of artificial intelligence and blockchain technology. These approaches aim to ensure data security, authenticity, and privacy while addressing scalability challenges and improving system performance. However, they also pose their own set of complexities and considerations, highlighting the need for ongoing research and development in this field.

Conclusion and Prospects

This study has primarily explored the application scenarios of privacy protection technologies amalgamated with artificial intelligence and blockchain, elucidating their associated methodologies while evaluating five critical characteristics. Furthermore, it has identified deficiencies within current systems and proposed recommendations for enhancement. Finally, these technologies have been categorized and summarized based on application scenarios and technical solutions. This research provides valuable insights for the advancement of AI and blockchain fusion and offers novel perspectives and directions for future exploration.

Despite significant strides, challenges persist in the realm of privacy protection technologies built upon the fusion of AI and blockchain, particularly in striking a balance between privacy preservation and data sharing. Exploring the fusion of AI and blockchain privacy protection technologies remains a promising research avenue. Consequently, we outline several approaches to integrate other techniques:

1. Edge Computing: Leveraging edge devices for processing private data facilitates decentralization in edge computing. Given the substantial computational resources required for AI processing, incorporating edge computing enables the distribution of computational tasks to edge devices, reducing transmission latency and network congestion while enhancing system processing speed and performance.

2. Multi-chain Mechanisms: Multi-chain mechanisms have the potential to address single-chain blockchain performance and storage limitations, thereby enhancing system scalability. Integrating multi-chain mechanisms enables data classification based on distinct attributes and privacy levels, thereby improving the security and storage capabilities of privacy protection systems.

References

[1]. Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, 21260 (2008).

[2]. Binance, "Bitcoin price," Available at: https://www.binance.com/en/price/bitcoin (2023).

[3]. Xiao Li, "Hybrid analysis of smart contracts and malicious behaviors in Ethereum," Hong Kong Polytechnic University, 179 (2021).

[4]. Prithviraj Mukherjee, Chandan Pradhan, "Blockchain 1.0 to blockchain 4.0—the evolutionary transformation of blockchain technology," In Blockchain Technology: Applications and Challenges, Springer, pp. 29–49 (2021).

[5]. Christian Schaefer, Christian Edman, "Transparent logging with Hyperledger Fabric," In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, pp. 65–69 (2019).

[6]. H. S. Jennath, V. S. Anoop, S. Asharaf, "Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence," International Journal of Interactive Multimedia and Artificial Intelligence, 6, 1–9 (2020).

[7]. Xianwei Tang, Lu Zhu, Ming Shen, Jianwei Peng, Jun Kang, Dusit Niyato, Abdelgadir A. A. El-Latif, "Secure and trusted collaborative learning based on blockchain for artificial intelligence of things," IEEE Wireless Communications, 29 (3), 14–22 (2022).

[8]. Wei Li, Jiajun Bu, Xiaodong Li, Xiaoyun Chen, "Security analysis of DeFi: Vulnerabilities, attacks and advances," In Proceedings of the IEEE International Conference on Blockchain (Blockchain), IEEE, pp. 488–493 (2022).

[9]. Francisco J. de Haro-Olmo, Ángel J. Varela-Vaca, José A. Álvarez-Bermejo, "Blockchain from the perspective of privacy and anonymisation: A systematic literature review," Sensors, 20 (24), 7171 (2020).

[10]. Bin Zhang, Jing Zhu, Hao Su, "Toward the third generation artificial intelligence," Scienc China Information Sciences, 66 (2), 121101 (2023).

[11]. Xiao Li, Tian Chen, Xiangfeng Luo, Tao Zhang, Lei Yu, Zhenhua Xu, "Stan: Towards describing bytecodes of smart contract," In Proceedings of the IEEE International Conference on Software Quality, Reliability and Security (QRS), IEEE, pp. 273–284 (2020).

[12]. Adnan Wasay, Suman Chatterjee, Stratos Idreos, "Deep learning: Systems and responsibility," In Proceedings of the International Conference on Management of Data (COMAD), ACM, pp. 2867–2875 (2021).

[14]. Veronin, M. A., Schumaker, R. P., & Dixit, R. (2020). The irony of MedWatch and the FAERS database: an assessment of data input errors and potential consequences. *Journal of Pharmacy Technology*, *36*(4), 164-167.
https://doi.org/10.1177/8755122520928

[15]. Veronin, M. A., Schumaker, R. P., Dixit, R. R., Dhake, P., & Ogwo, M. (2020). A systematic approach to'cleaning'of drug name records data in the FAERS database: a case report. *International Journal of Big Data Management*, *1*(2), 105-118.

https://doi.org/10.1504/IJBDM.2020.112404

[16]. Schumaker, R. P., Veronin, M. A., & Dixit, R. R. (2022). Determining Mortality Likelihood of Opioid Drug Combinations using Decision Tree Analysis. https://doi.org/10.21203/rs.3.rs-2340823/v1

[17]. Schumaker, R. P., Veronin, M. A., Dixit, R. R., Dhake, P., & Manson, D. (2017). Calculating a Severity Score of an Adverse Drug Event Using Machine Learning on the FAERS Database. In *IIMA/ICITED UWS Joint Conference* (pp. 20-30). INTERNATIONAL INFORMATION MANAGEMENT ASSOCIATION.

[18]. Dixit, R. R. (2018). Factors Influencing Healthtech Literacy: An Empirical Analysis of Socioeconomic, Demographic, Technological, and Health-Related Variables. *Applied Research in Artificial Intelligence and Cloud Computing*, *1*(1), 23-37.

[19]. Dixit, R. R. (2022). Predicting Fetal Health using Cardiotocograms: A Machine Learning Approach. *Journal of Advanced Analytics in Healthcare Management*, *6*(1), 43-57. Retrieved from https://research.tensorgate.org/index.php/JAAHM/article/view/38

[20]. Dixit, R. R. (2021). Risk Assessment for Hospital Readmissions: Insights from Machine Learning Algorithms. *Sage Science Review of Applied Machine Learning*, *4*(2), 1-15. Retrieved from https://journals.sagescience.org/index.php/ssraml/article/view/68

[21]. Ravi, K. C., Dixit, R. R., Singh, S., Gopatoti, A., & Yadav, A. S. (2023, November). AI-Powered Pancreas Navigator: Delving into the Depths of Early Pancreatic Cancer Diagnosis using Advanced Deep Learning Techniques. In *2023 9th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSS58085.2023.10407836

[22]. Khan, M. S., Dixit, R. R., Majumdar, A., Koti, V. M., Bhushan, S., & Yadav, V. (2023, November). Improving Multi-Organ Cancer Diagnosis through a Machine Learning Ensemble Approach. In *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1075-1082). IEEE. https://doi.org/10.1109/ICECA58529.2023.10394923

[23]. Sarker , M. (2023). Assessing the Integration of AI Technologies in Enhancing Patient Care Delivery in U.S. Hospitals. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 338-351. https://doi.org/10.60087/jklst.vol2.n2.p351

[24]. Yi Zhang, Shuang Li, Yufeng Shi, Xuan, et al., "Secure multi-party θ-join algorithm toward data federation," Chinese Journal of Software, 34 (3), 1109 (2023).

[25]. Andrew C. Yao, "Protocols for secure computations," In Proceedings of the IEEE Annual Symposium on Foundations of Computer Science (FOCS), IEEE, pp. 160–164 (1982).

[26]. Cynthia Dwork, "Differential privacy," In Proceedings of the International Colloquium

on Automata, Languages and Programming (ICALP), Springer, pp. 1–12 (2006).