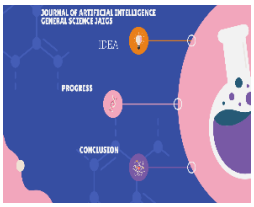
Vol.3, Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS

Home page http://jaigs.org




# Privacy-Preserving Architectures for AI/ML Applications: Methods, Balances, and Illustrations

Harish Padmanaban

Site Reliability Engineering lead and Independent Researcher

*Corresponding Author: Harish Padmanaban

***ARTICLEINFO***
***Article History:***
*Received: 05.03.2024*
*Accepted: 10.03.2024*
*Online: 02.04.2024*
***Keyword:*** Artificial Intelligence; Blockchain Privacy Protection; Data Encryption; De-identification; Access Control

*ABSTRACT*

With the widespread integration of artificial intelligence (AI) and blockchain technologies, safeguarding privacy has become of paramount importance. These techniques not only ensure the confidentiality of individuals' data but also maintain the integrity and reliability of information. This study offers an introductory overview of AI and blockchain, highlighting their fusion and the subsequent emergence of privacy protection methodologies. It explores various application contexts, such as data encryption, de-identification, multi-tier distributed ledgers, and k-anonymity techniques. Moreover, the paper critically evaluates five essential dimensions of privacy protection systems within AI-blockchain integration: authorization management, access control, data security, network integrity, and scalability. Additionally, it conducts a comprehensive analysis of existing shortcomings, identifying their root causes and suggesting corresponding remedies. The study 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 resulting from the integration of AI and blockchain, emphasizing the need to enhance efficiency and security for a more comprehensive safeguarding of privacy.

# Introduction:

In recent years, the fusion of Artificial Intelligence (AI) and Machine Learning (ML) technologies has reshaped various industries, fostering innovation and enhancing efficiency. Nevertheless, as reliance on AI/ML applications grows, concerns surrounding data privacy and security have taken center stage. With organizations accumulating vast troves of sensitive data for training and deploying AI models, safeguarding privacy has become an imperative challenge.

To tackle these concerns, there's been a surge of interest in privacy-preserving AI/ML application architectures. These architectures aim to deploy robust techniques and strategies to shield sensitive data while leveraging AI and ML capabilities for insights and decision-making. Thus, grasping the array of techniques, trade-offs, and real-world case studies becomes crucial for organizations eyeing the adoption of privacy-preserving AI/ML solutions.

This paper delves into the intricate realm of privacy-preserving AI/ML application architectures, exploring a spectrum of techniques employed to uphold data privacy while upholding the effectiveness of AI/ML models. From encryption methodologies to differential privacy frameworks, each technique carries its distinct trade-offs, striking a balance between privacy necessities and considerations of performance and usability.

Moreover, the paper scrutinizes real-world case studies spanning various industries, illustrating how organizations have effectively deployed privacy-preserving AI/ML application architectures to tackle specific challenges. These case studies offer valuable insights into the practical implications, hurdles encountered, and key takeaways from implementing privacy-preserving AI/ML solutions.

By synthesizing cutting-edge research, industry best practices, and practical experiences, this paper aims to provide a comprehensive panorama of privacy-preserving AI/ML application architectures. It empowers readers with the knowledge and insights necessary to navigate the intricate landscape of privacy protection in AI/ML applications, enabling organizations to make informed decisions and craft robust privacy-preserving strategies for their AI endeavors.

**Privacy and Security in AI and Blockchain**

**1. Evolution of Blockchain Technology**

The emergence of the Bitcoin blockchain system, introduced by Nakamoto in November 2008 [1], ignited global interest and sparked extensive discussions. The exponential surge in Bitcoin's value has propelled the term "cryptocurrency" into the forefront of both industrial and academic discourse. As of February 18, 2023 [2], Bitcoin's circulating market capitalization reached RMB 3.25 trillion, underscoring its substantial commercial significance and the vast potential of virtual currencies within the financial domain. This surge has revitalized research and development efforts in blockchain technology. The initial phase, dubbed Blockchain 1.0, primarily hinges on distributed ledgers. The advent of Ethereum in 2014 marked a pivotal juncture in Blockchain 2.0, integrating groundbreaking technologies such as smart contracts [3]. Blockchain 3.0 has introduced application platforms for the Internet of Things and smart healthcare [4], while Blockchain 4.0 aims to forge a resilient ecosystem and broaden the applications of blockchain technology across diverse sectors, including culture, entertainment, and communication infrastructure [5].

Blockchains are classified based on their accessibility and governance levels, chiefly as public, private, and federated chains. Public blockchains like Bitcoin and Ethereum epitomize decentralization, facilitating free entry and exit of nodes, thereby fostering maximum decentralization. Federated chains, exemplified by FISCO BCOS [6], enable smart contract execution using Turing-complete languages and employ homomorphic cryptography for privacy protection, albeit with partial decentralization. Conversely, private blockchain networks such as Antchain regulate node permissions while offering expedited transaction processing and reduced fees.

The structure of the Ethereum blockchain, depicted in Figure 1, employs a linked list data structure to interlink multiple blocks [7]. Each block header retains the hash address of the preceding block, ensuring a sequential linkage between successive blocks. Despite the manifold advantages of blockchain technology, security concerns across various domains cannot be disregarded. In the financial sector, the economic repercussions of privacy breaches are immeasurable [8]. Safeguarding user assets and identity information has become paramount in blockchain security research, given their criticality and the potential menace posed by malevolent nodes. Security remains an indispensable facet of any industry or technology, with blockchain security being pivotal for its sustainable progression.

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

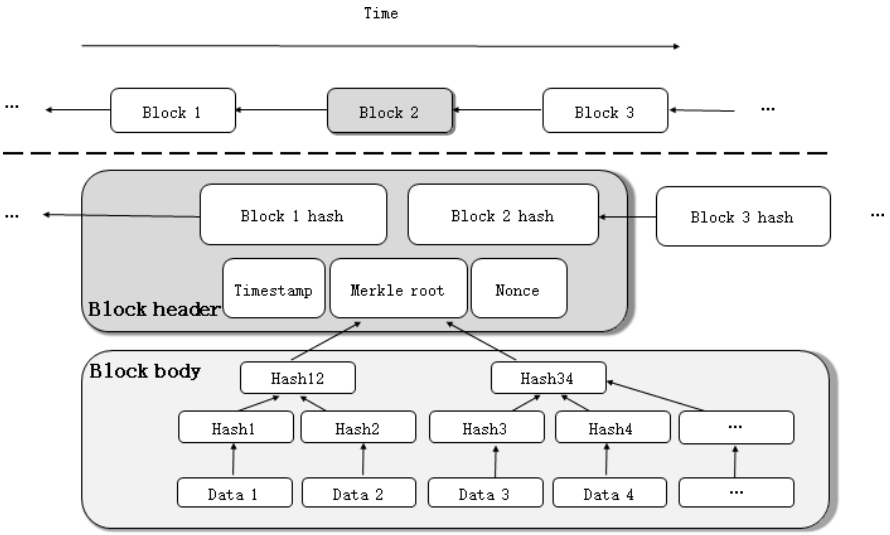



Figure 1: Structure of the Ethereum Blockchain

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).

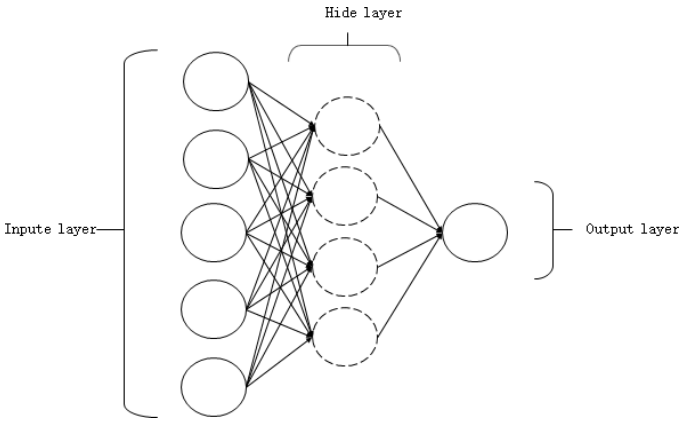
## 2. Artificial Intelligence

Artificial intelligence (AI) [10] is a discipline dedicated to crafting computer systems capable of mimicking autonomous thought processes and decision-making. The primary objective of AI is to render informed judgments and proficiently execute predefined tasks. Recent groundbreaking achievements, such as DeepMind's AlphaGo claiming the world champion title and the success of OpenAI's ChatGPT model, have propelled AI into the limelight, eliciting substantial interest globally. Subdomains within AI encompass deep learning, natural language processing (NLP), and others, all interconnected by their core mission of scrutinizing and deciphering data.

Natural Language Processing (NLP) [10] stands as a vital subfield of AI concerned with processing various forms of textual and linguistic data. Advancements in deep learning have engendered the development of cutting-edge NLP models like BERT and GPT. NLP employs specialized processing techniques or models to computationally dissect data, facilitating tasks such as text categorization, speech recognition, and machine translation.

The initial phase of NLP entails converting text into a format comprehensible by computers. However, this endeavor is complicated by language intricacies, ambiguity, and the necessity for precise evaluation metrics. Researchers tackle these complexities by employing specific symbolic representations and neural network architectures tailored to different NLP tasks.

Deep Learning (DL) [12] serves as a cornerstone of AI, modeled after the neural structure of the human brain. DL processes input information through hierarchical network structures, layer by layer, to generate a final representation. It encompasses supervised and unsupervised learning methodologies and has profoundly influenced domains such as image processing, speech recognition, and NLP.




In Figure 2, deep learning (DL) employs a multi-level neural network architecture to extract data features. This neural network consists of three primary types of layers: the input layer, the hidden layer, and the output layer. Each layer of perceptrons is interconnected, forming the deep learning model. The emergence of distributed deep learning has made computational parameters such as eigenvalues and gradient values crucial information transmitted between nodes during model training. However, the existence of malicious nodes poses a threat as they could intercept computation results using sophisticated attack algorithms, potentially leading to the exposure of sensitive data through reverse inference or data leakage.

## 3. Convergence of Artificial Intelligence and Blockchain Technologies

In today's era of information technology, the fusion of artificial intelligence (AI) and blockchain technologies is increasingly prevalent across various sectors, emphasizing the importance of addressing data security and privacy concerns. Pioneering initiatives such as Anthropic's Constitutional AI [13], SingularityNET's Decentralized AI [14], and ChainLink's Decentralized Oracle [15] exemplify the deep integration of AI and blockchain technologies, aiming for enhanced efficiency, security, and transparency in data processing.

Anthropic's Constitutional AI system leverages large-scale models and blockchain technologies to ensure audit tracking and accountability throughout the model training process, covering data, parameters, and outputs. Similarly, SingularityNET's Decentralized AI system implements AI models on blockchain networks, fostering decentralized collaboration and services among models. This setup enables users to conveniently access models, adjust parameters, and utilize highly dependable 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, thus furnishing a credible external information source for blockchains.

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

1. Utilization of blockchain technology for storing and recording 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. Provision of secure access to external AI models and data through decentralized systems, empowering blockchain networks to access reliable external information.

4. Harnessing blockchain-based incentive mechanisms and token designs to establish incentivized connections and trust interactions between AI model developers and users.

## Blockchain Privacy Protection

Blockchain technology, renowned for its distributed ledger system and consensus algorithms like Proof of Stake (PoS) [16], guarantees on-chain data integrity and transaction encryption through cryptographic methods. However, despite its inherent transparency, the exposure of sensitive data on the blockchain poses significant challenges to data privacy and security [17], particularly in domains like financial applications and supply chain management, where transaction data confidentiality holds paramount importance. To tackle these challenges and expand the horizons of blockchain applications, ensuring robust data security and privacy protection becomes imperative.

Numerous data protection technologies have been proposed to bolster data privacy on the blockchain, encompassing zero-knowledge proof, ring signatures, homomorphic encryption, and secure multi-party computation [18]. Each of these technologies offers distinctive capabilities in fortifying data privacy:

### Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP), a cryptographic technique introduced by Goldwasser et al. [19] in 1985, enables a prover to demonstrate the correctness of a statement to a verifier without disclosing any information beyond the

statement's validity. In the blockchain context, ZKP protocols like zk-SNARKs are widely utilized to ensure privacy by generating succinct proofs without divulging underlying data, facilitating functionalities such as decentralized coin-mixing pools for enhanced privacy [20].

**Ring Signature**

Ring Signature (RS), conceived by Rivest in 2001 [21], permits a signer to conceal their identity within a group of users, forming a ring of participants of equal status. When applied to the blockchain, RS obscures transaction addresses, rendering it challenging for attackers to deduce traders' identities. By selecting members within the ring, users augment privacy, with variations such as threshold ring signatures offering additional flexibility and security.

**Homomorphic Encryption (HE)**

Homomorphic Encryption (HE) stands as a pivotal cryptographic technique in blockchain development, allowing operations on encrypted data without exposing plaintext, thereby ensuring both confidentiality and data availability. With partial and fully homomorphic encryption, users can securely perform computations on encrypted data, preserving privacy while upholding computational efficiency [22].

Each of these privacy protection technologies plays a crucial role in enhancing data privacy on the blockchain, mitigating concerns associated with confidentiality and security.

**Artificial Intelligence Privacy Protection Technology**

In the era of advanced AI technologies, safeguarding the privacy of sensitive personal data holds paramount importance, particularly in sectors such as healthcare and finance. With AI models evolving continuously, including language analysis and perception models like ChatGPT, preserving privacy while leveraging sensitive data becomes imperative. Various privacy protection techniques, such as secure multi-party computation and homomorphic encryption, play pivotal roles in ensuring the security of sensitive information across diverse AI applications.

**Secure Multi-party Computation (SMPC)**

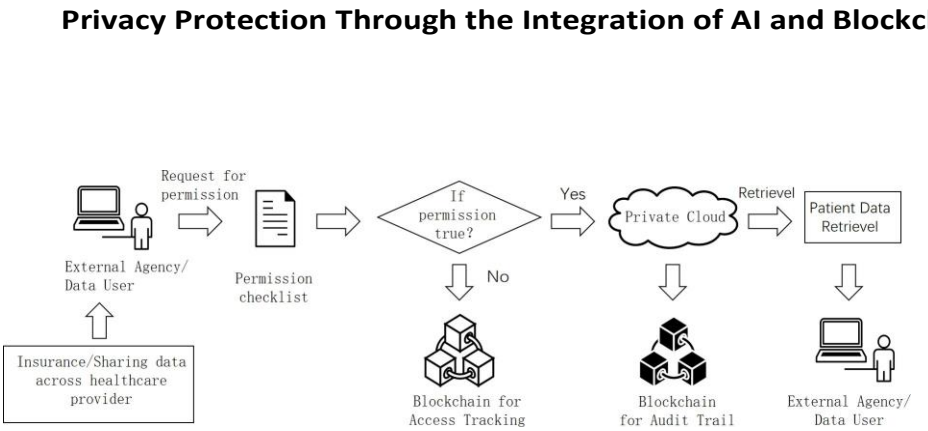
Secure Multi-party Computation (SMPC) enables multiple participants to collaboratively process private data without disclosing individual inputs. Protocols like garbled circuits and secret sharing facilitate secure computation of functions while maintaining data privacy, ensuring that each participant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

**Differential Privacy**

Differential privacy, introduced by Dwork et al. in 2006 [26], revolves around preserving data privacy by introducing controlled noise to sensitive information during data processing. By striking a balance between data distortion and

privacy requirements, differential privacy techniques guarantee that sensitive information does not unduly influence data queries, thus mitigating privacy risks while preserving data utility [27].

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




Currently, the reliability of data transmission within the data trust system faces limitations [28], posing risks to data security and privacy. To address this challenge, integrating blockchain technology can establish a robust and trustworthy data storage and sharing system, thereby enhancing data security and privacy protection [29]. Table 1 delineates specific applications of integrating artificial intelligence and blockchain in privacy protection technology. Strengthening the integration and deployment of these technologies can significantly augment the security and protective capabilities of the existing data trust system.

**Data Encryption**

Conventional data storage and sharing methods are vulnerable to various security threats [30][6][31], notably due to their dependence on centralized servers, rendering them susceptible to attacks and resulting in issues such as data leaks and tampering. Traditional encryption methods are inadequate to meet the escalating security requirements [34][35].

To address these challenges, privacy protection technology amalgamating artificial intelligence and blockchain has emerged. Leveraging distributed encryption algorithms substantially enhances the security and privacy protection level of data.

Given that traffic and vehicle data often encompass 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,

facilitating 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 functions as follows:**

(1) Key Generation: The process involves selecting two random large prime numbers $p$ and $q$ to satisfy $n_0$ and $\lambda$ as per Formula 2 and Formula 3, respectively. Then, a value $g$ is chosen from set $B$ to fulfill 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: The Paillier algorithm is applied using Formula 6.

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

(3) Decryption: The ciphertext $c$ is decrypted 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, $(n_0, g)$ denotes the public key, while $(\lambda, \mu)$ represents the private key. $m$ denotes the plaintext, and $r < n_0$ is a random number.

**De-identification**

De-identification serves as a widely adopted technique for anonymizing personal identification information within data by segregating data identifiers from the data itself, thus mitigating risks associated with data tracking. 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 facilitates the sharing of medical data without compromising patient identities. The framework utilizes two independent blockchains for data requests, as depicted 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 constitutes a decentralized data storage system comprising multiple hierarchical layers designed to facilitate efficient and secure data sharing while upholding privacy protection [31][7].

Chang et al. [31] introduced DeepLinQ, a blockchain-based multi-layer distributed ledger aimed at addressing users' privacy concerns regarding 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 facilitates privacy-protected distributed data sharing.

### K-anonymity

The K-anonymity method [37][38] constitutes a privacy protection technique focusing on grouping individuals in a dataset such that 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 is a critical security measure that regulates user access to authorized resources based on predefined rules or policies to maintain system security and data integrity. Therefore, designing and implementing access control mechanisms are of paramount importance in both blockchain and AI systems.

TURKI et al. [41] pioneered an intelligent privacy parking management system that leverages AI and blockchain technology, employing a Role-Based Access Control (RBAC) model for permission management [42, 43, 44, 50, 51, 52]. In 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] developed a privacy protection and intrusion detection framework grounded in blockchain and deep learning, outlining four levels of access control policies. The framework includes Membership Service Participants (MSPs) responsible for managing client registration, authentication processes, and issuance and storage of participant certificates. Additionally, Key Verifiers (KVs) verify user identities and certificates upon request.

**Access Control**

Access control is pivotal in ensuring privacy protection by regulating access based on user identity and group membership to ensure only authorized users can access specific resources, thus protecting the system from unauthorized intrusion. Effective access control requires meticulous consideration and implementation of factors such as user authentication [41], authorization [48], and access policies [42]. Only through integrating these aspects can privacy and security be maintained within the system.

Digital Identity Technology (DIT) [40, 41, 42, 48, 53] emerges as a promising approach for IoT applications, providing secure access control and safeguarding device and data privacy. Wazid et al. [47] proposed access control policies based on digital identity technology and cryptographic primitives to enhance communication security among entities like drones, Ground Station Servers (GSS), and cloud servers. This approach ensures secure data sharing.

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

Despite advancements, some systems still struggle to implement effective access control. Table 4 summarizes deficiencies and implicated layers. Potential reasons include unreasonable system design and inadequate permission control, leading to security vulnerabilities.

**Data Protection**

Data protection encompasses various measures such as access control, data encryption [40, 54], data backup, and security auditing to prevent illegal access, tampering, or leakage of user data. Technologies like anonymization [42], data masking [46], data encryption, and data isolation [55] shield data from unauthorized access and leakage. Encryption technologies like differential privacy protection [45], homomorphic encryption [49], hash algorithms [42, 47], digital signature algorithms [49], and asymmetric encryption algorithms [46, 48] ensure data confidentiality and prevent unauthorized access.

Wan et al. [45] utilized homomorphic encryption to encrypt local model parameters of edge devices before uploading them to the central server. This study integrated differential privacy protection to safeguard privacy.

Lee et al. [48] introduced a management framework leveraging blockchain and AI technology to safeguard the privacy of digital assets, utilizing OrbitDB as an off-chain distributed database. This approach ensures data security and privacy, preventing data abuse.

However, reliance solely on encryption technology is insufficient for data protection. Table 5 outlines issues related to data protection, including heavy reliance on blockchain for security and difficulties in designing encryption algorithms for real-world scenarios.

**Network Security**

Network security encompasses preventing network attacks, ensuring data confidentiality and integrity, and safeguarding systems from malicious software and network viruses. Various security measures, secure network architectures, and protocols must be implemented to achieve system security and reliability [57].

Ali et al. [49] proposed a privacy-preserving intrusion detection framework based on blockchain and deep learning. This framework incorporates an Intrusion Detection System (IDS) that monitors and analyzes network traffic, identifying intrusions using feature-based and anomaly-based methods.

Singh et al. [40] introduced an IoT healthcare privacy protection framework integrating federated learning and blockchain technology, enhancing security with protocols in IoT devices and intelligent systems.

Table 6 outlines network attacks and preventive measures for privacy protection systems. The absence of network security protection may lead to various security threats and risks, causing significant losses to individuals and businesses. Therefore, ensuring network security protection is crucial in privacy protection systems integrating artificial intelligence and blockchain.

**Scalability**

Scalability refers to a system's capacity to accommodate an increasing number of users or larger data volumes. When designing for scalability, factors such as system performance, node management, data storage, and transmission must be carefully considered to ensure that scalability is achieved without compromising security.

Lee et al. [48] developed a system compliant with the European General Data Protection Rules (GDPR) by storing artwork metadata and privacy-related data in a distributed file system off the blockchain. Digital tokens and artwork metadata are stored in OrbitDB, a distributed database across multiple nodes, enhancing system scalability by dispersing data storage.

Wan et al. [45] introduced a blockchain-based B5G edge device privacy protection framework utilizing federated learning for 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 risks of single-point failure and poisoning attacks. This framework's versatility allows for application across various datasets, models, computing resources, and algorithms, enhancing system scalability while improving model interpretability and effectively managing bias and noise.

Many systems lack adequate scalability design or rely excessively on blockchain's distributed nature, facing challenges such as scaling issues, low transaction processing speeds, and interoperability problems. Techniques like distributed storage, computing, data sharding, and parallel processing can enhance scalability. In privacy protection systems integrating AI and blockchain, scalability is crucial due to processing extensive volumes of sensitive data, necessitating careful consideration to ensure continuous and stable system operation.

**Situation Analysis**

The fusion of blockchain technology and AI has led to the development of systems effectively safeguarding user privacy data. Challenges including data protection, access control, network security, and scalability must be comprehensively addressed during the design phase based on practical considerations.

Privacy protection applications leveraging AI and blockchain technology can be categorized into three main groups: IoT applications, smart contracts and services, and large-scale data analysis techniques. Each category focuses on distinct aspects of privacy protection, leveraging the combined strengths of AI and blockchain while addressing scalability challenges and improving system performance. Ongoing research and development are necessary to address complexities and considerations in this evolving field.

## Conclusion and Outlook

This study has delved into the diverse application scenarios of privacy protection technologies amalgamated with artificial intelligence (AI) and blockchain, elucidating their methodologies and evaluating critical characteristics. It has also identified deficiencies in current systems and proposed recommendations for improvement. Finally, the study has categorized and summarized these technologies based on their application scenarios and technical solutions, providing valuable insights for advancing the fusion of AI and blockchain and offering novel perspectives for future exploration.

Despite significant progress, challenges persist in the domain of privacy protection technologies integrating AI and blockchain, particularly in balancing privacy preservation with data sharing. Exploring the fusion of AI and blockchain for privacy protection remains a promising research avenue. Consequently, several approaches can be considered for further integration:

1. Edge Computing: Utilizing edge devices for processing private data facilitates decentralization in edge computing. With the substantial computational resources required for AI processing, integrating edge computing allows

distributing computational tasks to edge devices. This reduces transmission latency and network congestion while enhancing system processing speed and performance.

2. Multi-chain Mechanisms: Implementing multi-chain mechanisms can address performance and storage limitations of single-chain blockchains, thereby enhancing system scalability. By integrating multi-chain mechanisms, data can be classified based on distinct attributes and privacy levels, improving the security and storage capabilities of privacy protection systems.

## References

[1]. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 189-208. DOI: https://doi.org/10.60087/jaigs.v2i1.p208

[2]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 47-66. DOI: https://doi.org/10.60087/jaigs.v1i1.p66

[3]. Li, Z., Huang, Y., Zhu, M., Zhang, J., Chang, J., & Liu, H. (2024). Feature Manipulation for DDPM based Change Detection. *arXiv preprint arXiv:2403.15943*.

https://doi.org/10.48550/arXiv.2403.15943

[4]. Ramírez, J. G. C. (2023). Incorporating Information Architecture (ia), Enterprise Engineering (ee) and Artificial Intelligence (ai) to Improve Business Plans for Small Businesses in the United States. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 115-127. **DOI:** https://doi.org/10.60087/jklst.vol2.n1.p127

[5]. Ramírez, J. G. C. (2024). AI in Healthcare: Revolutionizing Patient Care with Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 31-37. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p37

[6]. Ramírez, J. G. C. (2024). Natural Language Processing Advancements: Breaking Barriers in Human-Computer Interaction. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 31-39.**DOI:** https://doi.org/10.60087/jaigs.v3i1.63

[7]. Ramírez, J. G. C., &mafiqul Islam, M. (2024). Application of Artificial Intelligence in Practical Scenarios. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19. **DOI:** https://doi.org/10.60087/jaigs.v2i1.41

[8]. Ramírez, J. G. C., & Islam, M. M. (2024). Utilizing Artificial Intelligence in Real-World Applications. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19.

DOI: https://doi.org/10.60087/jaigs.v2i1.p19

[9]. Ramírez, J. G. C., Islam, M. M., & Even, A. I. H. (2024). Machine Learning Applications in Healthcare: Current Trends and Future Prospects. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1). **DOI:** https://doi.org/10.60087/jaigs.v1i1.33

[10]. RAMIREZ, J. G. C. (2023). How Mobile Applications can improve Small Business Development. *Eigenpub Review of Science and Technology*, *7*(1), 291-305. **https://studies.eigenpub.com/index.php/erst/article/view/55**

[11]. RAMIREZ, J. G. C. (2023). From Autonomy to Accountability: Envisioning AI's Legal Personhood. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(9), 1-16. https://researchberg.com/index.php/araic/article/view/183

[12]. Ramírez, J. G. C., Hassan, M., & Kamal, M. (2022). Applications of Artificial Intelligence Models for Computational Flow Dynamics and Droplet Microfluidics. *Journal of Sustainable Technologies and Infrastructure Planning*, *6*(12).https://publications.dlpress.org/index.php/JSTIP/article/view/70

[13]. Ramírez, J. G. C. (2022). Struggling Small Business in the US. The next challenge to economic recovery. *International Journal of Business Intelligence and Big Data Analytics*, *5*(1), 81-91. https://research.tensorgate.org/index.php/IJBIBDA/article/view/99

[14]. Ramírez, J. G. C. (2021). Vibration Analysis with AI: Physics-Informed Neural Network Approach for Vortex-Induced Vibration. *International Journal of Responsible Artificial Intelligence*, *11*(3).https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/77

[15]. Shuford, J. (2024). Interdisciplinary Perspectives: Fusing Artificial Intelligence with Environmental Science for Sustainable Solutions. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 1-12.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p12

[16]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[17]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[18]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[19]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[20]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[21]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[22]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

**DOI:** https://doi.org/10.60087/jaigs.v2i1.p47

[23]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[24]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[25]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[26]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[27]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273.

[28]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[29]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572317_Critical_study_of_software_models_used_cloud_application_development/links/65ad55d7ee1e1951fbd79df6/Critical-study-of-software-models-used-cloud-application-development.pdf

[30]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572222_Implication_of_Artificial_Intelligence_in_Software_Development_Life_Cycle_A_state_of_the_art_review/links/65ad54e5bf5b00662e333553/Implication-of-Artificial-Intelligence-in-Software-Development-Life-Cycle-A-state-of-the-art-review.pdf

[31]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[32]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.https://patents.google.com/patent/US20230385176A1/en

**[33]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.DOI: https://doi.org/10.60087/jklst.vol2.n3.p412**

**[34]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence.https://shodhganga.inflibnet.ac.in/handle/10603/487443**

**[35]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89. DOI: https://doi.org/10.60087/jaigs.v2i1.p89**

**[36].** Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

DOI: https://doi.org/10.60087/jaigs.v3i1.75

[37]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[38]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[39]. Ara, A., &Mifa, A. F. (2024). INTEGRATING ARTIFICIAL INTELLIGENCE AND BIG DATA IN MOBILE HEALTH: A SYSTEMATIC REVIEW OF INNOVATIONS AND CHALLENGES IN HEALTHCARE SYSTEMS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(01), 01-16.

DOI: https://doi.org/10.62304/jbedpm.v3i01.70

[40]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.
DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[41]. Bappy, M. A. (2024). Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review. *American Journal of Science and Learning for Development*, *3*(2), 11-21.
DOI: https://doi.org/10.51699/ajsld.v3i2.3459

[42]. Uddin, M. N., Bappy, M. A., Rab, M. F., Znidi, F., &Morsy, M. (2024). Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications.
DOI: https://doi.org/10.5772/intechopen.114168

[43]. Hossain, M. I., Bappy, M. A., &Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64

[44]. Zhu, M., Zhang, Y., Gong, Y., Xing, K., Yan, X., & Song, J. (2024). Ensemble Methodology: Innovations in Credit Default Prediction Using LightGBM, XGBoost, and LocalEnsemble. *arXiv preprint arXiv:2402.17979*.

https://doi.org/10.48550/arXiv.2402.17979

[45]. Yafei, X., Wu, Y., Song, J., Gong, Y., & Lianga, P. (2024). Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(2), 11-20.

DOI: https://doi.org/10.60087/jklst.vol.3n2.p20

[46]. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. *Academic Journal of Science and Technology*, *10*(1), 299-304.

https://drpress.org/ojs/index.php/ajst/article/view/19205

[47]. Ness, S., Sarker, M., Volkivskyi, M., & Singh, N. (2024). The Legal and Political Implications of AI Bias: An International Comparative Study. *American Journal of Computing and Engineering*, *7*(1), 37-45.
DOI: https://doi.org/10.47672/ajce.1879

[48]. Sarker, M. (2022). Towards Precision Medicine for Cancer Patient Stratification by Classifying Cancer By Using Machine Learning. *Journal of Science & Technology*, *3*(3), 1-30.
DOI: https://doi.org/10.55662/JST.2022.3301

[49]. Manoharan, A., & Sarker, M. REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION.

DOI : https://www.doi.org/10.56726/IRJMETS32644