A Security-Centric Perspective on AI and Blockchain Integration with Network Infrastructure Security in 5G and IoT Edge Environments

Omkar Singh* and Col. Rahul Sharma

National Institute of Fashion Technology, Patna, Bihar, India
Email: omkar.singh@nift.ac.in (O.S.); colrahul.sharma@nift.ac.in (R.S.)
*Corresponding author
Manuscript received May 28, 2025; accepted June 24, 2025; published August 21, 2025

***Abstract*—With blockchain technology and Artificial Intelligence (AI) coming together, the digital world is changing quickly and opening up new possibilities for secure, autonomous, and decentralized systems. This paper examines the integration of these disruptive technologies from a security perspective, examining how they might enhance data integrity, privacy, and trust, particularly in light of new network infrastructures like 5G and Internet of Things (IoT) edge settings. The study examines the security flaws in blockchain and Artificial Intelligence (AI) alone and together, highlighting how combining the two can both increase and decrease risks. The difficulties of protecting information and computation across dispersed, low-latency edge nodes in 5G-enabled IoT systems are specifically discussed. The report outlines the main dangers, real-world applications, and future research avenues needed to create reliable and scalable AI-blockchain frameworks for contemporary communication networks. It concludes that strong approaches to interoperability, secure edge deployment, governance, and infrastructure resilience are necessary to fully realise the potential of these technologies.**

***Keywords*—Artificial Intelligence (AI), blockchain, applications, challenges, solutions, attacks**

I. Introduction

Two ground-breaking technologies that have become quite popular in the twenty-first century are blockchain and Artificial Intelligence (AI). While AI focuses on empowering machines to carry out activities that normally require human intellect, blockchain offers a decentralised, tamper-proof ledger for recording digital transactions [1]. Building autonomous, secure, and intelligent systems is made possible by their convergence, particularly when applied to cutting-edge infrastructures like 5G networks and Internet of Things (IoT) edge devices, where secure communication and real-time decision-making are crucial. Strong security measures are essential to preventing data leaks, illegal access, and hostile manipulation as AI systems spread throughout edge computing environments made possible by 5G [2]. At the same time, blockchain applications are expanding beyond cryptocurrencies into industries like finance, supply chain management, and healthcare, all of which depend more and more on edge computing for processing data with low latency [3]. Blockchain integration can provide safe, decentralised data sharing, and Artificial Intelligence (AI) improves real-time threat detection and anomaly prediction.

Both blockchain and artificial intelligence have built-in security flaws, notwithstanding their advantages. AI models are susceptible to inference assaults, data poisoning, and privacy abuses. Despite being decentralised, blockchain has problems with scalability, 51% assaults, and defects in smart contracts [4]. These concerns are exacerbated in the case of 5G/IoT edge networks due to the dispersed nature of devices and the requirement for constant, low-latency connections. Some of these issues can be resolved, though, by carefully combining blockchain with AI. For example, blockchain can safely store and validate data produced by edge AI models, while AI can instantly identify dangers like malicious smart contract activity or device compromise [5].

With an emphasis on implementation inside contemporary network infrastructures, this study investigates the integration of AI with blockchain from a security-first standpoint. After providing an overview of the fundamental technological concepts of blockchain and artificial intelligence, it focuses the security issues with each technology separately and in combination [6]. Their use in 5G-enabled IoT environments, where latency, bandwidth, and trust management become crucial considerations, is highlighted. The study examines real-world applications, identifies unresolved research issues, and suggests future paths for creating robust digital ecosystems via this integration [7]. The layered integration model of blockchain and AI across network edges is depicted in Fig. 1.

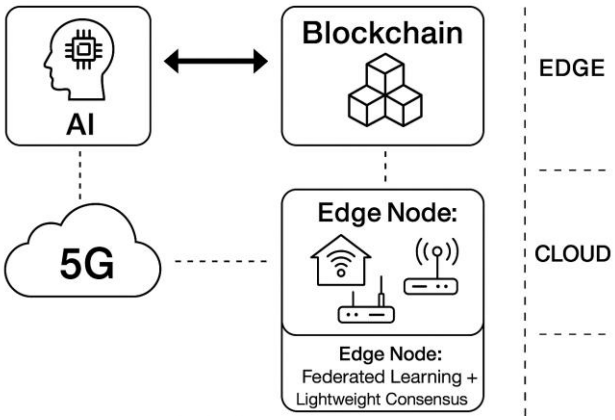

Fig. 1. Integration of technologies.

A. Motivation of the Research

An intriguing new approach to addressing significant security concerns in modern digital ecosystems is provided by the combination of blockchain technology and Artificial Intelligence (AI). In 5G networks and IoT edge environments, where enormous amounts of data are created, processed, and sent in real time across dispersed nodes, this

integration becomes even more crucial. Even while AI continues to revolutionize automation, data processing, and decision-making, it also poses hazards such as data manipulation, hostile attacks, and privacy infringement [8]. While blockchain offers a decentralized, unchangeable framework that can improve data integrity, transparency, and trust, it also has drawbacks in terms of scalability, energy consumption, and smart contract vulnerabilities. The unique chance to combine the advantages of blockchain and Artificial Intelligence (AI) to create intelligent, dependable, and secure systems, especially in latency-sensitive, high-speed 5G and IoT edge deployments, is what drives this study [9]. Organizations may reduce the risks associated with each technology by combining the analytical capabilities of AI with the reliable architecture of blockchain. Innovations like auditable AI judgements, decentralized intelligence at the edge, and safe, impenetrable data sharing across several infrastructures are made possible by this partnership [10].

B. Key Contributions of the Article

The key contributions of the article are as follows:

- The study thoroughly examines the distinct security issues that arise from blockchain and artificial intelligence separately, as well as the heightened risks and weaknesses that arise from their combination.
- It offers a conceptual framework that demonstrates how blockchain technology and Artificial Intelligence (AI) can complement one another's security aspects, such as enhanced data integrity, safe model management, and decentralized trust.
- The study adds to the expanding corpus of adversarial threat modelling by identifying new attack vectors unique to AI-blockchain systems, such as model poisoning through smart contracts and AI-driven exploitation of blockchain consensus.
- This study examines real-world AI-blockchain integration systems, weighing their advantages and disadvantages from a security perspective.
- Applications and network attacks based on various technologies are discussed.

II. Background and Literature Review

A vast array of technologies that seek to mimic or reproduce human intelligence in machines is collectively referred to as artificial intelligence. These include robots, computer vision, Natural Language Processing (NLP), deep learning, and Machine Learning (ML) [11]. The capacity of machine learning and deep learning to learn from data and generate predictions or judgments with little assistance from humans makes them especially noteworthy. Advances in autonomous driving, language translation, and picture identification have been made possible by recent developments in neural networks, particularly deep learning [12]. Concern over AI security is growing. Since models are frequently trained on huge datasets, they are susceptible to hostile inputs and data manipulation. Furthermore, many AI models—also known as "black boxes"—are opaque, making it hard to validate or explain their choices, which undermines responsibility and confidence [13].

Blockchain is a distributed ledger technology that guarantees decentralization, transparency, and immutability. It makes it possible to permanently and verifiably record transactions without depending on a centralized authority. To create a safe chain, each block in a blockchain includes a timestamp, transaction data, and a cryptographic hash of the previous block [14]. Blockchain was first envisioned as the technology behind Bitcoin, but it has since found uses in a variety of fields, including digital identity verification, supply chain management, and medical record management. The usefulness of blockchain has been further increased by smart contracts, which are self-executing agreements with stipulations encoded directly into the code [15]. Blockchain has several security problems despite its advantages. If inaccurate or malicious information is captured, the immutability of data may turn into a liability. It is possible to exploit smart contracts if they are not properly coded and audited. Proof-of-Work (PoW) and other consensus techniques are energy-intensive and vulnerable to 51% assaults [16].

Numerous academic and commercial initiatives have investigated the combination of blockchain technology and artificial intelligence. Singularity NET and other decentralized AI markets, for example, seek to offer a platform where blockchain technology may be used to access and monetize AI services. In a similar vein, initiatives such as Ocean Protocol use blockchain-based access constraints to enable safe and transparent data exchange amongst AI models [17]. According to published research, there is increasing interest in leveraging blockchain technology to improve data provenance, auditability, and AI model integrity. On the other hand, artificial intelligence is being used more and more to improve blockchain functions, including transaction validation, anomaly detection, and consensus mechanism improvement. Deeper research is necessary because there are yet few thorough studies on the security implications of this integration [18].

Even though both technologies have advanced considerably, their integration is still in its infancy, especially when it comes to security. Standardized frameworks for safe AI-blockchain implementations are scarce [19]. Other urgent issues are scalability, regulatory compliance, and interoperability. To create safe, integrated platforms, the literature points to the necessity of interdisciplinary approaches that integrate knowledge from distributed systems, machine learning, and cybersecurity [20]. A review summary is shown in Table 1:

Table 1. Review summary

Aspect	Background	Review
Purpose [21]	Introduces the fundamental concepts of AI, Blockchain, and their relevance to security.	Provides a detailed analysis of existing studies, methodologies, and findings related to AI-blockchain security.
Content Focus [22]	Explains basics of AI and blockchain technology, highlighting their potential and challenges.	Surveys previous research works, identifies gaps, and discusses current security challenges and solutions.
Scope [23]	Broad overview of the two technologies and their general applications in security contexts.	Specific to prior academic and practical contributions focused on integrating AI with blockchain securely.

Depth [24]	Introductory and explanatory, aimed at readers unfamiliar with the detailed technicalities.	Analytical and critical, comparing different approaches and identifying limitations in existing research.
Security Perspective [25]	Introduces the importance of security concerns in AI and blockchain separately and combined.	Examines how security has been addressed in AI-blockchain systems, highlighting strengths and weaknesses.
Key Themes [26]	Definitions, technological components, historical context, and motivation for integration.	Techniques used for AI security, blockchain vulnerabilities, hybrid system designs, and emerging threats
References Used [27]	General sources on AI and blockchain technology fundamentals and security principles.	Specific research articles, case studies, surveys, and experimental results relevant to AI-blockchain security.
Role in Paper [28]	Sets the stage by establishing foundational knowledge and justifying the study's importance.	Builds a framework for the study by synthesizing existing knowledge and identifying research gaps.
Outcome [29]	Readers gain understanding of why AI and blockchain integration is critical for security.	Readers understand what has been done and where further research is needed in AI-blockchain security integration.

III. Technological Applications

When paired with secure 5G and IoT edge infrastructures, the combination of blockchain and Artificial Intelligence (AI) opens up a plethora of revolutionary applications. In addition to improving operational effectiveness, these apps tackle important security issues in trustworthy communication, decentralised decision-making, and real-time data processing. Ten noteworthy applications are listed below:

A. Autonomous Transportation Networks

Autonomous vehicles are guided by AI models, and blockchain records interactions, navigation choices, and maintenance information. 5G enables quick connectivity between infrastructure and automobiles. This configuration guards against malicious control signals, Global Positioning System (GPS) manipulation, and spoofing [11].

B. Intelligent Supply Chain and Logistics

Blockchain keeps tamper-proof supply records, AI forecasts delays or interruptions, and IoT edge devices track items in real time. Manufacturers, carriers, and retailers can coordinate easily thanks to the 5G infrastructure [13].

C. Smart Grid and Energy Systems

Blockchain controls peer-to-peer energy trades, I predict patterns in energy consumption, and edge IoT devices keep an eye on nearby grids. 5G secures the system, preventing data manipulation and guaranteeing the dependability of renewable energy sources and smart meters [15].

D. Decentralized Identity and Access Control

Edge AI processes biometric data locally, and blockchain securely stores and verifies IDs. Real-time, secure authentication is guaranteed by 5G connection for applications such as public services, finance, and e-governance [16].

E. Industrial IoT (IIoT) Automation

Blockchain keeps track of maintenance logs and audit trails, while Edge AI keeps an eye on machinery and anticipates malfunctions. In industrial settings, 5G ensures cybersecurity and uninterrupted operations by facilitating fast machine-to-machine connectivity [18].

F. Smart Cities and Infrastructure Management

5G guarantees quick data flow, blockchain records public occurrences, and AI systems handle environmental and surveillance data locally. This preserves data integrity and transparency while enhancing public safety, disaster response, and traffic management [20].

G. Disaster Response and Emergency Services

While blockchain securely records all operations, edge AI allows autonomous drones and rescue equipment to make judgments locally in disaster areas. Even in difficult circumstances, 5G guarantees continuous communication [21].

H. Military and Tactical Communication Networks

5G enables quick unit coordination, blockchain guarantees safe command-and-control communication, and AI technologies offer combat analytics at the edge. This makes it possible for military networks in dangerous areas to be robust and impenetrable [23]. The various applications using different technologies are shown in Fig. 2.

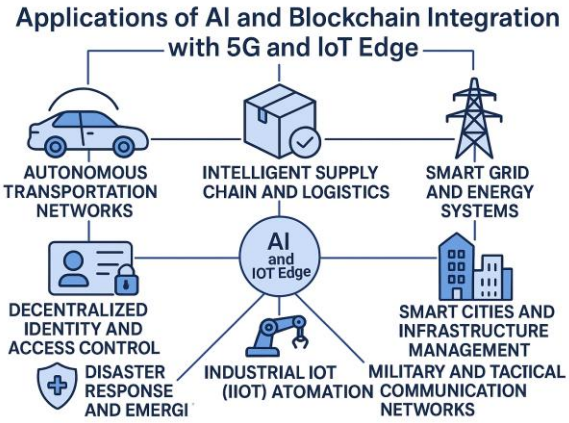

Fig. 2. Applications of different technologies.

IV. Security Challenges

A. Fashion Adversarial Attacks

The susceptibility of models to hostile attacks is among the most urgent security issues in AI. These attacks entail tampering with input data such that AI models generate inaccurate results that seem natural to humans. For instance, a facial recognition system may incorrectly identify a person if a few pixels in an image are changed. These minor disruptions can get beyond AI defenses, which presents significant risks in high-stakes industries like autonomous driving, healthcare, and finance [30].

B. Data Poisoning

Large amounts of training data are essential to AI systems. Data poisoning is a technique used by malicious actors to

introduce inaccurate or misleading data into training datasets. This may lead to biased or erroneous models that behave erratically or perform badly in real-world situations. Data poisoning can be used to create covert backdoors into AI systems in addition to compromising model reliability [31].

C. Privacy and Data Leakage

AI models are vulnerable to privacy abuses, especially those that were trained on private information. Sensitive data can be extracted from trained models using methods such as membership inference attacks and model inversion. This presents moral and legal issues, particularly in situations where data protection laws like the General Data Protection Regulation (GDPR) are in effect [32].

D. Model Theft and Reverse Engineering

AI models are a substantial investment in processing power and intellectual property. Model extraction attacks, in which an adversary searches the model and recreates its functionality, allow attackers to steal these models. Such theft increases the possibility of misuse or unauthorized replication in addition to jeopardizing competitive advantage [33].

E. Lack of Explainability and Accountability

A lot of sophisticated AI systems, especially deep learning models, operate as "black boxes" with no insight into how they make decisions. In regulated businesses, this lack of explainability makes it more difficult to identify mistakes, gain consumer trust, and adhere to legal obligations. Assigning culpability for detrimental judgements made by AI systems is challenging in the absence of explicit accountability [34].

F. Smart Contract Vulnerabilities

On blockchain networks, smart contracts are self-executing programs that automate intricate transactions. However, bad actors may take advantage of coding mistakes or faulty reasoning [35]. The DAO breach on Ethereum, which caused millions of dollars to be lost because of a reentrancy vulnerability, is one notable example. Because smart contracts are immutable, any vulnerabilities may be irreversible once they are deployed because they cannot be readily changed [36, 37].

G. Privacy Limitations

Blockchain offers transparency, but there are privacy issues as well. Every transaction is recorded on public blockchains so that all users can see it. Even if identities are pseudonymous, people can frequently be de-anonymized by advanced research. Applications that need secrecy, such financial transactions or medical records, may find this lack of privacy troublesome [38].

H. Scalability and Performance Bottlenecks

Blockchain networks frequently experience performance and scalability problems, especially those that use Proof-of-Work. The amount of time and computing power needed to handle transactions rises with their volume. Denial-of-Service (DoS) attacks, which try to overload the network and impair its functionality, can be used to take advantage of these bottlenecks [39].

I. Key Management Risks

Cryptographic keys are essential to blockchain's identity and access control. Unauthorized access to private data or the irretrievable loss of assets can arise from the loss, theft, or compromise of private keys. Inadequate key management procedures pose a serious risk, especially for small businesses with weak security measures and individual users [40].

J. Distributed Attack Surface

There are more possible entry points for attackers because of the dense infrastructure of 5G base stations and the decentralised nature of IoT edge devices. This complicates the process of identifying and containing threats [36].

K. Data Integrity and Privacy Risks

If not sufficiently secured, sensitive data processed at the edge may be intercepted, changed, or leaked. When integrating blockchain-based logs and AI models across the edge, it becomes imperative to ensure secure data provenance and end-to-end encryption [41, 42].

L. Device Authentication and Trust Management

It becomes difficult to confirm the authenticity and integrity of devices when millions of edge devices are dynamically connecting. Inadequate authentication procedures can result in spoofing, impersonation, or the infiltration of rogue devices [38].

M. Low-Latency Exploitation

Ultra-low latency communication is made possible by 5G, but it also leaves little time for conventional security procedures. Attackers can use this quick data flow to initiate low-detection, high-speed attacks like DoS attacks or real-time inference altering [27].

N. Resource Constraints at the Edge

Because edge devices frequently have low processing and memory capacities, it is difficult to implement computationally demanding security measures like blockchain consensus, deep encryption, or real-time AI-based anomaly detection [33].

O. Smart Contract and AI Model Vulnerabilities

If smart contracts in blockchain-enabled IoT devices are not adequately validated, they could be abused. In a similar vein, hostile inputs can be used to attack edge-deployed AI models, resulting in inaccurate or manipulated choices [28].

P. Network Slicing Risks in 5G

Network slicing is supported by 5G to separate services; nevertheless, if isolation is not adequately enforced, vulnerabilities in one slice may be exploited to impact others, increasing the risk of cross-slice data breaches or service interruption [29].

Security challenges in AI and Blockchain are summarized in Table 2.

Table 2. Summarizing security challenges in AI and Blockchain

Security Challenge	AI-Specific Issues	Blockchain-Specific Issues	Challenges in AI-Blockchain Integration
Data Privacy [41]	AI requires large datasets, risking exposure of sensitive data during training and inference.	Blockchain's immutable ledger conflicts with privacy laws (e.g., GDPR's right to be forgotten).	Balancing immutable ledgers with AI's need for data updates and privacy compliance.
Data Integrity [42]	AI models can be poisoned by malicious data inputs, causing wrong predictions or decisions.	Blockchain ensures data integrity but smart contract bugs can corrupt processes.	Coordinated attacks targeting both AI training data and blockchain transactions.
Adversarial Attacks [43]	AI models vulnerable to adversarial inputs that manipulate outputs.	Blockchain networks vulnerable to 51% attacks or Sybil attacks affecting consensus.	Exploiting AI vulnerabilities to manipulate blockchain consensus or decision-making.
Model Security [44]	AI models can be stolen or reverse-engineered, leaking intellectual property or sensitive patterns.	Blockchain smart contracts are immutable and bugs cannot easily be patched.	Difficulty updating AI models deployed on immutable blockchain infrastructure.
Scalability and Performance [45]	AI computation-intensive; requires high processing power and latency-sensitive responses.	Blockchain consensus and transaction processing are slow and resource-heavy (e.g., PoW).	Combined overheads can limit real-time AI-blockchain applications, reducing usability.
Consensus Security [46]	Not applicable to AI alone.	Vulnerable to malicious nodes or collusion undermining trust in network decisions.	Ensuring AI outputs are validated and trusted within decentralized blockchain consensus.
Transparency and Explainability [47]	AI's black-box nature makes decision processes opaque, raising trust concerns.	Blockchain offers transparency but can expose sensitive business logic or data.	Reconciling AI's opaque models with blockchain's open ledger transparency requirements.
Regulatory Compliance [48]	AI systems struggle with compliance due to dynamic, opaque decision-making.	Blockchain's immutability complicates data modification and privacy regulation adherence.	Designing compliant AI-blockchain systems respecting privacy, transparency, and data laws.
Energy Consumption [49]	AI training and inference can be energy-intensive, especially deep learning models.	Blockchain PoW consensus consumes significant energy.	Combined environmental impact raises sustainability challenges.
Trust and Adoption [50]	Skepticism around AI's reliability and ethical concerns can hinder trust.	Blockchain's complexity and scalability issues affect enterprise adoption.	User trust depends on secure, transparent, and performant integrated systems.

V. Synergies and Security Benefits

A. Enhanced Threat Detection and Response

Blockchain's capacity to identify and address security problems can be enhanced by AI. Real-time blockchain transaction monitoring using machine learning algorithms allows systems to spot unusual trends that could be signs of fraud or an attack. AI-based Intrusion Detection Systems (IDS), for instance, are able to identify anomalous transaction patterns or questionable wallet activity and start automated reactions [51].

B. Secure Data Sharing and Federated Learning

Blockchain can let dispersed AI systems share data in a transparent and safe manner. In federated learning, where several entities train a common AI model without disclosing raw data, this is especially advantageous. Blockchain lowers the possibility of data loss and tampering by guaranteeing the integrity and traceability of participant contributions and model modifications [52].

C. Improved Model Integrity and Auditability

The integrity and auditability of AI models can be improved by storing model hashes or version histories on the blockchain. This method makes it simpler to confirm the legitimacy and dependability of AI outputs—a crucial aspect in regulated industries—by producing unchangeable records of model deployments, revisions, and the origin of training data [53].

D. Decentralized AI Marketplaces

Blockchain makes it possible to build decentralized marketplaces for AI services and models where users may communicate with one another without the need for centralized middlemen. AI can provide equitable matching and recommendation systems, while smart contracts control licensing, payments, and usage rights. These platforms lessen the possibility of central points of failure and encourage openness [54].

E. AI-Enhanced Blockchain Security

By constantly modifying factors like mining difficulty or validator selection in response to current network conditions, Artificial Intelligence (AI) can optimize blockchain consensus mechanisms. AI algorithms can also be used to anticipate possible network congestion or denial-of-service attacks and take preemptive measures to lessen their effects [55].

F. Trustworthy Autonomous Systems

When creating autonomous systems that need to function safely in changing surroundings, including drones, cars, and Internet of Things gadgets, blockchain and artificial intelligence must be integrated. AI makes it possible for intelligent, context-aware behavior, while blockchain offers tamper-proof records of choices and activities. When combined, they promote transparency, accountability, and reliability in self-governing activities [56].

G. Dynamic, Scalable Security Frameworks

Adaptive security policies are made possible by 5G's software-defined capabilities and dynamic network management. These can be paired with blockchain for

verifiable enforcement and AI for predictive threat response, creating adaptable and scalable trust frameworks [41].

H. Trust Anchors for Intelligent Automation

Blockchain auditing of AI models operating on edge nodes can guarantee openness and equity in automated decision-making. Verifiable logs that promote accountability and traceability are produced via blockchain-based hashes of model versions and inference outcomes [42].

VI. Network Attacks

The potential for intelligent, decentralised, and real-time applications is huge when Artificial Intelligence (AI) and Blockchain are integrated with cutting-edge network infrastructure like 5G and IoT edge settings. But this convergence also creates a new set of intricate vulnerabilities by greatly increasing the network attack surface. In such systems, the following primary attack vectors are particularly pertinent [20]:

A. Sybil Attacks

Sybil attacks in blockchain networks entail the construction of a large number of phoney nodes in order to obtain an excessive amount of control over consensus processes. Malicious actors may infiltrate or impersonate numerous edge devices when applied to 5G and IoT edge environments, hence penetrating blockchain validation networks and AI model pipelines. These assaults have the potential to distort AI training datasets and erode confidence in consensus findings [21].

B. 51% Attacks

A 51% assault gives enemies control over most of the blockchain's processing capacity, allowing them to double-spend or modify transactions. Blockchain systems operating at the edge, frequently with fewer validators, make localised 51% attacks conceivable. These attacks can be combined with AI to create secure data histories in decentralized systems or alter decision logs [33].

C. Data Poisoning

Data poisoning, in which adversaries introduce false or malicious data to taint the learning process, can affect AI models, particularly those at the edge. Sensors in IoT-based environments may be compromised to provide AI systems with inaccurate data. A chain reaction of persistent, difficult-to-correct disinformation is produced when such tainted material is likewise irreversibly recorded onto the blockchain [22].

D. Adversarial Input Attacks

In order to trick AI networks into incorrectly classifying or interpreting data, adversaries can gently alter inputs. This could entail manipulating sensor streams, biometric information, or camera feeds in an edge environment. In a blockchain-controlled system, these deceptive inputs may cause inaccurate smart contract executions, leading to unexpected outcomes [35].

E. Man-in-the-Middle (MitM) Attacks

MitM attacks provide serious concerns in the communication channel between blockchain nodes, edge devices, and AI inference engines. Attackers have the ability to intercept and change smart contract payloads, inference findings, and critical training data. The absence of secure routing protocols can leave data vulnerable to illegal access or modification in 5G environments, where speed and latency are top priorities [26].

F. Denial-of-Service (DoS/DDoS) Attacks

Both blockchain and AI services require a lot of compute and are availability-sensitive. DoS attacks are especially dangerous for edge networks with limited resources. Attackers can stop or taint blockchain validation and AI decision flows in a 5G setting by overloading edge servers or AI models with requests, which can result in system breakdowns or latency spikes [37].

G. Cross-Slice Attacks in 5G

Network slicing, or the virtual division of services for various applications, is made possible by 5G architecture. Because of inadequate isolation measures, attackers may switch across slices if one is compromised. The trust boundaries of logically independent infrastructures may be compromised by coordinated attacks on blockchain ledgers and AI models spread across various slices [28].

Through the integration of blockchain-based attestation methods and AI-driven isolation, the presented framework improves the security of 5G network slicing. Unauthorised lateral movements across slices can be dynamically detected and prevented by using AI approaches to monitor slice-specific behaviour. At the same time, blockchain guarantees unchangeable and verifiable access logs, strengthening accountability and confidence in cross-slice conversations. This two-pronged strategy offers real-time threat response, enhances traceability, and fortifies slice borders. Consequently, in intricate, multi-tenant 5G systems, the architecture provides a strong defence against coordinated cross-slice attacks. The Slice Specific Security Framework is shown in Fig. 3.

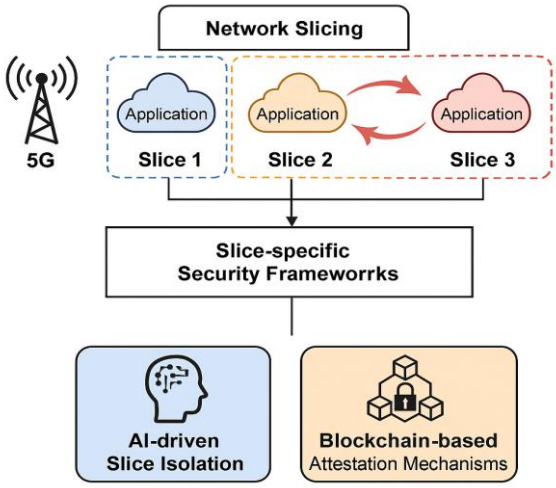

Fig 3. Slice specific security framework.

H. Replay and Routing Attacks

Attackers have the ability to record valid transactions or inference outcomes and then replay them to skew system states or initiate out-of-date actions. The timing sensitivity of blockchain event sequences or AI judgements can be further distorted by malicious or flawed edge routing, which

compromises system reliability overall [30].

I. Eavesdropping and Data Leakage

Because 5G radio access and edge networks are wireless, passive threats like eavesdropping are frequent. The privacy and integrity of blockchain and AI systems can be jeopardised by adversaries who can intercept encrypted payloads, blockchain credentials, or training data [39].

J. Smart Contract Exploits

In IoT environments, smart contracts can be activated by AI results or real-world data. Unauthorised or antagonistic inputs could cause contracts to perform unexpected actions. Therefore, AI-generated data, particularly from unreliable or tainted sources, can be used to influence blockchain behaviour, including making incorrect access control decisions or transferring funds without authorisation [44].

The Summarization of network attacks are shown in Table 3.

Table 3. Summarizing network attacks

Attack Type	Description	Targeted Layer	Security Impact
Sybil Attack [21]	Creation of fake nodes/devices to manipulate blockchain consensus or AI models	Blockchain, Edge Nodes	False consensus, poisoned training data, trust compromise
51% Attack [33]	Attacker controls majority of blockchain computation	Blockchain at Edge	Double-spending, data tampering
Data Poisoning [35]	Insertion of malicious data into AI training pipelines	AI at Edge, IoT Sensors	Corrupt AI models, faulty predictions
Adversarial Input Attack [26]	Small perturbations to input cause AI misclassification	AI Inference Engines	Incorrect decisions, smart contract misuse
Man-in-the-Middle (MitM) [37]	Interception of data between AI, IoT, and blockchain components	5G Channels, IoT Gateways	Data manipulation, privacy loss
DoS/DDoS Attack [28]	Overloading edge nodes or validators with traffic	AI/Blockchain Nodes, 5G Infrastructure	Service unavailability, delayed responses
Cross-Slice Attack [30]	Pivoting between 5G slices due to poor isolation	5G Network Slicing	Breach of isolated services, data leakage
Replay Attack [39]	Reuse of legitimate data/transactions to confuse systems	Blockchain, AI Logs	State inconsistency, unauthorized actions
Smart Contract Exploits [44]	Triggering unintended behavior via adversarial inputs	Blockchain, AI-Connected Contracts	Unauthorized operations, trust erosion

VII. Case Study: AI-Blockchain Integrated 5G Smart Factory under Security Attack

A. Context

A city hospital implemented a cutting-edge AI-assisted diagnostic system that was connected to 5G-enabled IoT edge devices (such as wearable monitoring and smart infusion pumps) and blockchain for patient data integrity. The system was designed to offer remote monitoring, safe patient data exchange, and real-time diagnostics.

B. Security Incident

In order to create false cardiac alerts, an attacker took advantage of a flaw in an AI model that was installed at the edge (on wearable ECG monitors) and fed it hostile data. At the same time, unauthorised access to patient data that had been stored was obtained by abusing a smart contract vulnerability in the blockchain-based access control system. This caused linked infusion pumps to do automatic actions, such changing dosages incorrectly.

C. Root Cause

- Lack of secure AI model validation at the edge allowed tampering.
- Blockchain smart contracts lacked dynamic patching mechanisms.
- Non-standardized APIs between the 5G core and edge controllers delayed threat detection and containment.
- Limited computing power at the edge made real-time AI anomaly detection and consensus verification impractical.

D. Outcome

Inaccurate alerts were sent to a number of patients, and treatment delays happened. Despite the fact that there were no fatalities, the episode generated severe issues about compliance and trust. For auditing and recovery purposes, the hospital temporarily shut down its associated infrastructure.

E. Lessons Learned

- There is a critical need for energy-efficient, verifiable AI models at the edge.
- Smart contract auditing and update mechanisms must be integrated.
- Standardized, secure API frameworks for SDN/NFV-based networks are essential for fast response.
- Cross-network collaboration mechanisms should be strengthened for real-time mitigation.

VIII. Limitations and Open Challenges

Although there are several security benefits to combining blockchain technology with artificial intelligence, there are also significant operational, conceptual, and technical difficulties. Researchers, developers, and politicians must be aware of these constraints to create systems that are not only creative but also safe and useful [57].

A. Computational Overheads and Scalability

The combined processing overhead is a major issue when integrating blockchain and AI. While blockchain processes, especially those requiring consensus methods like Proof-of-Work (PoW), are resource-intensive, AI algorithms, particularly deep learning models, require a significant amount of computing power. Combining these technologies can increase latency and impede scalability, which makes it challenging to process and make decisions in real time, particularly in settings like financial trading platforms or autonomous systems [58].

B. Data Storage and Bandwidth Limitations

Blockchain's block size and storage cost restrictions make it unsuitable for storing massive amounts of data.

However, to learn and draw conclusions, AI systems frequently need access to large datasets. It is ineffective and impractical to try to store or maintain AI datasets directly on-chain. Although Interplanetary File System (IPFS) and other off-chain storage options have been proposed, they add further levels of complexity and possible points of attack [59].

C. Security Paradoxes and Attack Surfaces

While blockchain and AI integration improve security in certain ways, it also increases the attack surface overall. Model poisoning and adversarial attacks are two ways to corrupt AI models that are included in blockchain applications. On the other hand, AI operations may be compromised by taking advantage of flaws in smart contracts or blockchain technology. Coordinated assaults that take advantage of flaws in both systems at the same time, like data poisoning through a corrupted smart contract, are a new class of dangers that need more research [60].

D. Interoperability and Standardization

A major obstacle to broad adoption is the incompatibility of various blockchain platforms and AI frameworks. While AI systems are constructed using a variety of tools and libraries, each blockchain may have its distinct protocols, consensus techniques, and data structures. The deployment of cross-platform apps, data interchange, and integration activities is all made more difficult by this heterogeneity. For blockchain and AI components to work together seamlessly, standardized middleware, ontologies, and APIs are required [61].

E. Ethical and Regulatory Challenges

Complex ethical and legal questions are brought up by the combination of blockchain technology with AI. For example, storing AI decision logs or personal data on immutable ledgers may violate privacy laws such as the GDPR, especially the right to be forgotten. Furthermore, the use of AI to decentralized governance mechanisms (like DAO decision-making) could result in convoluted accountability chains and opaque procedures. It takes careful consideration of both technical design and legal frameworks to ensure fairness, transparency, and compliance in such hybrid systems [62].

F. Energy Consumption and Environmental Impact

Blockchain technology's effects on the environment, particularly those of PoW-based systems, are widely known. Significant energy resources are also needed for AI inference and training [63]. These technologies have the potential to increase carbon footprints when combined, which raises questions about sustainability. Even if energy-efficient AI models (like pruning and quantization) and alternative consensus mechanisms (like Proof-of-Stake) are being developed, the current integration status could not be in line with international sustainability goals [64].

G. Trust and Adoption Barriers

Although there are theoretical advantages to integrating AI and blockchain, industry maturity, consumer awareness, and trust issues prevent widespread implementation [65]. Businesses may be hesitant to implement integrated systems because of concerns about long-term viability, perceived complexity, or unclear return on investment. Implementation efforts are further slowed down by the high learning curve and lack of experts in both blockchain and artificial intelligence [66].

H. Research Gaps and Theoretical Foundations

Robust theoretical frameworks to direct safe AI-blockchain integration are scarce. In the context of hybrid architectures, important topics including safe multiparty computation, differential privacy, federated learning, and zero-knowledge proofs are still not well understood [67]. Furthermore, the absence of integrated environment-specific benchmarking datasets and simulation tools makes it challenging to verify security claims and performance measurements [68].

I. Governance and Decentralized Control

Blockchain-managed decentralized AI systems may have governance problems, especially in settings where several stakeholders with competing interests need to work together [69]. In such contexts, version control, conflict resolution, and system update mechanisms are intricate and little understood. While crucial, governance models that strike a balance between decentralization and efficient oversight are still mostly at the experimental stage [70].

J. Scalability

There are serious scalability challenges when integrating blockchain and AI in 5G and IoT edge scenarios. High computing resources are needed for AI models, while latency is introduced by blockchain consensus procedures. AI pipelines may be overloaded by the vast amounts of data from IoT devices. The throughput of blockchain is constrained for processing in real time. Both technologies are frequently too much for edge devices to handle well. Large-scale, low-latency deployment across vital industries is hampered by these limitations [57].

K. Cross-Network Collaboration

One of the biggest obstacles to smooth cross-network collaboration in integrated AI, Blockchain, 5G, and IoT edge systems is still present. Network interoperability is hampered by disparate standards, protocols, and latency-sensitive situations. It is difficult for edge nodes and blockchain validators to coordinate in real time. Decision-making may become fragmented as a result of inconsistent data synchronisation. Also lacking is cross-domain trust management. Strong governance procedures and consistent frameworks are needed to remove these obstacles [59].

L. Future-Proofing Against Emerging Threats

AI and blockchain systems need to adjust to preserve their security postures as quantum computing and next-generation cyberthreats change. Important topics for further study include adaptive security techniques, robust model generalization, and post-quantum cryptography [71]. Proactive investment is necessary to ensure that integrated systems continue to be resilient in the face of these new challenges [72]. Limitations and open challenges are shown in Table 4.

Table 4. Limitations and open challenges

Synergy/Benefit	Description	Security Implications
Enhanced Data Integrity [73]	Blockchain's immutable ledger ensures AI training and inference data remain tamper-proof.	Prevents data tampering and ensures trustworthy AI outputs by verifying data provenance.
Decentralized AI Model Management [74]	Distributing AI models on blockchain avoids centralized points of failure and censorship.	Improves resilience against attacks targeting AI infrastructure; enhances availability.
Improved Transparency and Auditability [75]	Blockchain provides a transparent record of AI decision-making processes and data usage.	Enables audit trails for AI model decisions, fostering accountability and trustworthiness.
Secure Federated Learning [76]	Blockchain can coordinate decentralized AI training across multiple parties without sharing raw data.	Preserves data privacy while enabling collaborative model improvements with secure aggregation.
Automated and Trusted Smart Contracts [77]	AI-powered smart contracts enable automated decision-making with adaptive learning capabilities.	Enhances contract execution accuracy and reduces fraud or manipulation risks.
Enhanced Privacy Preservation [78]	Combining AI techniques (e.g., differential privacy) with blockchain's cryptographic protocols.	Protects sensitive data in decentralized systems, supporting compliance with data privacy laws.
Robust Threat Detection [66]	AI analyzes blockchain transactions and network behavior to identify fraudulent or malicious actions.	Early detection and mitigation of security threats improves system robustness.
Data Monetization with Security [69]	Blockchain enables secure, traceable data exchanges; AI extracts value from this data efficiently.	Secure data marketplaces maintain user control and prevent unauthorized data access or misuse.
Resistance to Single Point of Failure [79]	Distributed blockchain infrastructure complements AI's reliance on centralized data or models.	Enhances system uptime and security by eliminating single points vulnerable to attack or failure.
Trustworthy AI Governance [80]	Blockchain-based decentralized autonomous organizations (DAOs) can govern AI lifecycle management.	Transparent, consensus-driven governance reduces risks of bias, manipulation, or unauthorized changes.

IX. Conclusion

A revolutionary change in the security, management, and optimization of digital systems is represented by the combination of blockchain technology and artificial intelligence. The combination of these technologies provides a compelling vision for the future of intelligent, secure systems, from improving the integrity of AI decision-making to enabling decentralized and tamper-resistant models of computation. But there are also significant complications brought forth by this convergence, like as rising storage and processing requirements, new security flaws, and regulatory issues.

This study has looked at the security issues with blockchain and artificial intelligence separately and together, emphasized the possible advantages of combining the two, and pointed out important gaps and unexplored areas. Although current use cases show promising applications in supply chain, cybersecurity, healthcare, and finance, scalability problems, ethical concerns, and the requirement for standardized interoperability frameworks continue to limit wider implementation.

The development of energy-efficient AI-blockchain consensus mechanisms specifically suited for low-power IoT edge devices, should be the main focus of future research. These techniques can preserve security while lowering computing overhead. To integrate blockchain, AI, and network functionalities like SDN controllers, it is necessary to standardise APIs. Interoperability between 5G and IoT ecosystems will be enhanced as a result. When combined, these guidelines can make cross-network collaboration scalable, lightweight, and safe. Real-time, robust digital infrastructure will require the establishment of universal frameworks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Omkar Singh has written and analyzed the manuscript, and Col. Rahul Sharma has reviewed the manuscript. Both authors have given the final approval for the manuscript.

References

[1] M. Ali, K. A. Shakil, and N. Aslam, "A comprehensive review of blockchain and AI applications in healthcare," *IEEE Access*, vol. 11, pp. 124557–124574, 2023.

[2] O. Singh and A. S. Kushwaha, "Improving energy efficiency in scalable WSNs through IoT-driven approach," *International Journal of Information Technology*, 2025. doi: 10.1007/s41870-025-02471-7

[3] U. Agarwal and V. Rishiwal, "Exploring blockchain and supply chain integration: State-of-the-art, security issues and emerging directions," *IEEE Access*, vol. 12, pp. 143945–143974, 2024.

[4] S. Singh and P. Yadav, "Localization in WSN-assisted IoT networks using machine learning techniques for smart agriculture," *International Journal of Communication Systems*, 2024. doi: 10.1002/dac.6004

[5] O. Singh, V. Rishiwal, and M. Yadav, "EPMR: Energy proficient mobile routing for scalable wireless sensor networks," *Wireless Personal Communications*, 2024. doi: 10.1007/s11277-024-11589-z

[6] P. Gupta and A. Singh, "Privacy preservation in AI-blockchain integration: Techniques and challenges," *Journal of Network and Computer Applications*, vol. 209, 103512, 2024.

[7] O. Singh and L. Kumar, "MLCEL: Machine learning and cost-effective localization algorithms for WSNs," *International Journal of Sensors, Wireless Communications and Control*, vol. 13, pp. 82–88, 2023.

[8] Y. Hu and X. Lin, "Adversarial attacks and defenses in AI-blockchain ecosystems," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1441–1454, 2024.

[9] V. Rishiwal and O. Singh, "Energy efficient emergency rescue scheme in wireless sensor networks," *International Journal of Information Technology*, 2020. doi: 10.1007/s41870-020-00584-9

[10] S. Jain and R. Kaur, "Blockchain and AI for secure data sharing in smart cities," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 348–357, 2024.

[11] O. Singh and V. Rishiwal, "Scalable energy efficient routing mechanism prolonging network lifetime in wireless sensor networks," *International Journal of Systems, Control and Communications*, vol. 11, no. 2, pp. 161–177, 2020.

[12] S. Kim and J. Park, "Blockchain-based decentralized AI model training: Security and privacy perspectives," *IEEE Access*, vol. 12, pp. 87456–87467, 2024.

[13] N. Kumar and R. Sharma, "AI-driven blockchain analytics for cyber threat intelligence," *Journal of Cybersecurity*, vol. 9, no. 1, 002, 2023.

[14] D. Lee and M. Choi, "Blockchain-backed explainable AI for secure decision-making," *Expert Systems with Applications*, vol. 213, 118806, 2024.

[15] F. Li and X. Zhao, "Blockchain and AI fusion for fraud detection: Current trends and future directions," *Information Processing & Management*, vol. 60, no. 6, 103728, 2023.

[16] H. Liu and K. Zhang, "Secure AI-powered blockchain consensus algorithms: A survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1215–1240, 2024.

[17] Y. Ma and D. Wang, "A survey on blockchain-based AI model sharing and privacy," *ACM Computing Surveys*, vol. 56, no. 4, 84, 2023.

[18] L. Meng and Y. Xu, "Quantum-resistant cryptography for AI-blockchain systems," *Quantum Information Processing*, vol. 23, no. 3, 89, 2024.

[19] K. Muhammad and S. U. Khan, "Hybrid AI-blockchain architectures for secure healthcare applications," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 6, pp. 2567–2577, 2023.

[20] V. Nair and S. Kumar, "Trust and accountability in AI-blockchain systems: Challenges and solutions," *Information Sciences*, vol. 636, pp. 407–423, 2024.

[21] D. Nguyen and T. Le, "Blockchain-based privacy-preserving AI models for edge computing," *IEEE Transactions on Mobile Computing*, vol. 22, no. 11, pp. 3234–3247, 2023.

[22] R. Oliveira and M. Santos, "AI-enhanced blockchain intrusion detection systems," *Journal of Network and Systems Management*, vol. 32, no. 1, 14, 2024.

[23] J. Park and Y. Kim, "Decentralized AI governance via blockchain," *Blockchain Research and Applications*, vol. 4, no. 4, 100125, 2023.

[24] S. Patel and N. Desai, "Enhancing blockchain security using deep reinforcement learning," *Neural Computing and Applications*, vol. 36, pp. 14257–14269, 2024.

[25] X. Qin and Z. Hu, "Blockchain-integrated AI for secure financial transactions," *Journal of Financial Innovation*, vol. 9, no. 2, 45, 2023.

[26] B. Ramesh and A. Srinivasan, "Privacy-preserving federated learning with blockchain for IoT networks," *Sensors*, vol. 24, no. 2, 456, 2024.

[27] S. Roy and A. Das, "Adversarial machine learning attacks on blockchain-enabled systems," *IEEE Security & Privacy*, vol. 21, no. 4, pp. 36–45, 2023.

[28] P. Sharma and S. Verma, "Blockchain and AI in cybersecurity: Current trends and future directions," *Computers & Security*, vol. 122, 102918, 2024.

[29] H. Singh and M. Kaur, "AI-based smart contract verification on blockchain," *Software Testing, Verification and Reliability*, vol. 33, no. 5, e2354, 2023.

[30] L. Sun and W. Zhang, "AI-blockchain integration for secure autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 3, pp. 975–987, 2024.

[31] J. Tan and M. Li, "AI-augmented blockchain for enhanced data privacy," *Journal of Network and Computer Applications*, vol. 205, 103418, 2023.

[32] Y. Wang and J. Zhou, "Blockchain-based trust management for AI models," *ACM Transactions on Internet Technology*, vol. 24, no. 1, pp. 1–22, 2024.

[33] C. Wu and L. Chen, "AI-driven blockchain forensics for enhanced security," *Digital Investigation*, vol. 40, pp. 301–312, 2023.

[34] Y. Xiao and J. Liu, "Secure blockchain-AI hybrid architectures for edge intelligence," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 5054–5066, 2024.

[35] D. Xu and Q. Yang, "Blockchain meets AI: A survey on decentralized AI and trust," *Information Fusion*, vol. 79, pp. 218–234, 2023.

[36] S. Yadav and P. Singh, "Enhancing blockchain security through AI-powered anomaly detection," *Future Generation Computer Systems*, vol. 148, pp. 284–296, 2024.

[37] F. Yang and H. Zhang, "Blockchain-enabled AI model provenance for data integrity," *Journal of Systems Architecture*, vol. 129, 102710, 2023.

[38] X. Yuan and H. Wang, "AI and blockchain for secure industrial IoT: Challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 1, pp. 219–228, 2024.

[39] R. Zhang and J. Li, "Secure multi-party computation with AI and blockchain for privacy preservation," *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 658–671, 2023.

[40] L. Zhao and Y. Sun, "Blockchain-based AI framework for secure smart grid management," *Energy Informatics*, vol. 7, no. 1, 17, 2024.

[41] S. Alotaibi and F. Alotaibi, "AI-powered blockchain analytics for fraud detection in cryptocurrency networks," *Journal of Information Security and Applications*, vol. 67, 103221, 2023.

[42] N. Aslam and M. K. Siddiqui, "Blockchain-based federated learning frameworks: Security and privacy perspectives," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 54–67, 2024.

[43] Q. Bai and Y. Liu, "Enhancing data privacy in AI-blockchain systems using homomorphic encryption," *Computers & Security*, vol. 125, 102970, 2023.

[44] J. Cao and L. Wei, "Blockchain-driven AI for secure medical data sharing," *Journal of Medical Systems*, vol. 48, no. 1, 10, 2024.

[45] M. Chen and C. Yang, "AI-blockchain integration for smart contract security: A survey," *IEEE Access*, vol. 11, pp. 45200–45215, 2023.

[46] W. Dai and X. Chen, "Secure and scalable AI model deployment on blockchain," *Future Generation Computer Systems*, vol. 155, pp. 345–359, 2024.

[47] S. Das and S. Saha, "Blockchain-based AI systems for supply chain integrity," *International Journal of Production Research*, vol. 61, no. 9, pp. 2701–2715, 2023.

[48] J. Eberhardt and S. Tai, "Blockchain-based trustworthy AI for decentralized finance," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 104–114, 2024.

[49] K. Fan and S. Wang, "AI-enabled blockchain for secure E-governance," *Government Information Quarterly*, vol. 40, no. 4, 101707, 2023.

[50] Y. Feng and P. Zhang, "Blockchain-assisted AI for cybersecurity threat intelligence sharing," *Computers & Security*, vol. 124, 102949, 2024.

[51] Z. Gao and H. Li, "AI and blockchain integration for privacy-preserving smart healthcare," *Journal of Healthcare Engineering*, vol. 2023, 8527632, 2023.

[52] A. Ghosh and P. Das, "Blockchain and AI for secure edge computing: A review," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1604–1627, 2024.

[53] D. He and D. S. Wong, "Blockchain-enhanced AI techniques for network intrusion detection," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1345–1356, 2023.

[54] X. Huang and Y. Shen, "AI-powered blockchain framework for secure IoT communications," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 5678–5689, 2024.

[55] M. Ibrahim and Y. Abushark, "Blockchain-based secure AI model sharing in collaborative environments," *IEEE Access*, vol. 11, pp. 29218–29231, 2023.

[56] S. Islam and M. Hassan, "Blockchain and AI for secure financial transactions: A deep learning approach," *Expert Systems with Applications*, vol. 222, 119528, 2024.

[57] Z. Jiang and X. Tan, "AI-driven blockchain model for fraud detection in financial markets," *Applied Intelligence*, vol. 53, pp. 5435–5450, 2023.

[58] J. Kang and J. Park, "A blockchain and AI combined approach for identity management," *Journal of Network and Computer Applications*, vol. 210, 103503, 2024.

[59] M. Khan and F. Ahmed, "AI-blockchain solutions for privacy preservation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 4, pp. 1019–1030, 2023.

[60] T. Kim and S. Lee, "Blockchain-based AI framework for secure data analytics," *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 3, pp. 847–859, 2024.

[61] M. Li and J. Chen, "Secure multi-agent systems using AI and blockchain technologies," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 5, pp. 3102–3114, 2023.

[62] Q. Liu and J. Wang, "Blockchain-enabled AI for privacy-preserving healthcare data analytics," *IEEE Journal of Biomedical and Health Informatics*, vol. 28, no. 2, pp. 875–886, 2024.

[63] L. Ma and X. Hu, "A survey on blockchain-based AI solutions for smart manufacturing security," *Computers in Industry*, vol. 145, 103673, 2023.

[64] H. Meng and Y. Zhou, "AI-enhanced blockchain frameworks for secure energy trading," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 888–899, 2024.

[65] A. Nawaz and H. Malik, "Blockchain and AI-driven intrusion detection systems: A comparative study," *Journal of Network and Computer Applications*, vol. 215, 103472, 2023.

[66] T. Nguyen and V. Tran, "Blockchain-assisted federated learning for IoT security: Challenges and solutions," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 4202–4215, 2024.

[67] Y. Pan and R. Zhao, "AI and blockchain integration for secure data provenance in cloud computing," *Future Generation Computer Systems*, vol. 150, pp. 70–82, 2023.

[68] K. Patel and R. Shah, "Blockchain-based AI framework for secure digital identity management," *Computers & Security*, vol. 127, 103047, 2024.

[69] X. Qian and J. Sun, "AI-powered blockchain for secure and transparent supply chains," *IEEE Transactions on Engineering Management*, vol. 70, no. 3, pp. 1110–1122, 2023.

[70] M. Rahman and M. Islam, "Blockchain and AI for privacy-preserving smart healthcare systems," *Journal of Medical Internet Research*, vol. 26, e45623, 2024.

[71] V. Reddy and P. Kumar, "AI-driven blockchain systems for fraud detection in banking," *Information Processing & Management*, vol. 60, no. 5, 103684, 2023.

[72] D. Roy and S. Chakraborty, "Blockchain-enabled AI for secure autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 6, pp. 5968–5980, 2024.
[73] F. Shao and M. Yang, "AI and blockchain for cyber threat intelligence sharing," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 68–74, 2023.
[74] A. Singh and R. Gupta, "Privacy-preserving AI and blockchain techniques for IoT networks," *Sensors*, vol. 24, no. 4, 1199, 2024.
[75] Y. Sun and D. Li, "Blockchain-based AI systems for enhancing cybersecurity in smart grids," *Energy Informatics*, vol. 6, no. 1, 24, 2023.
[76] Z. Tang and H. Liu, "AI-blockchain hybrid models for secure edge computing," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 2, pp. 1023–1035, 2024.
[77] F. Wang and T. Zhou, "Blockchain and AI for securing medical image data sharing," *Journal of Digital Imaging*, vol. 36, no. 3, pp. 695–705, 2023.
[78] L. Xu and Z. He, "AI-enabled blockchain for secure distributed cloud storage," *IEEE Transactions on Cloud Computing*, vol. 12, no. 1, pp. 99–110, 2024.
[79] S. Yoon and H. Park, "Blockchain-based AI framework for fraud detection in E-commerce," *Electronic Commerce Research and Applications*, vol. 54, 101149, 2023.
[80] X. Zhang and Y. Chen, "AI and blockchain integration for enhanced data privacy in financial services," *Journal of Financial Services Research*, vol. 66, no. 1, pp. 51–67, 2024.

Copyright © 2025 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).