

Integrating Blockchain, MQTT, and Machine Learning for Enhanced IoT Applications: A Comprehensive Survey

Maysaa Salama¹ 

¹Department of Computer Engineering, Sakarya University, Sakarya, Türkiye, ror.org/04ttnw109

Corresponding author:

Maysaa Salama
Computer and Information Engineering,
Sakarya University
E-mail address:
maysaa.salama@ogr.sakarya.edu.tr

Article History:

Received: 10.11.2024
Revised: 22.08.2025
Accepted: 25.08.2025
Published Online: 30.09.2025

ABSTRACT

This extensive research investigates the integration of blockchain, MQTT and machine learning on the Internet of Things (IoT), a field ripe for transformation with technologies. These three technologies are blockchain and Message Queuing Telemetry Transport (MQTT). Machine learning is a foundational pillar, each offering unique benefits to enhance data exchange, security and decision making in interconnected IoT environments. Our study aims to explore the synergies among these technologies and the implications of their combined usage on the IoT. I delve into how their integration strengthens data security, enables communication, and facilitates data-driven decision-making across IoT scenarios. The study examines types of blockchain technology and the significance of MQTT in IoT communication. Additionally, I explore the implementation of machine learning models. Our primary focus is on exploring how combining blockchain and MQTT can enhance data sharing. I address challenges such as privacy concerns, scalability issues and consensus processes. To illustrate the impact of this convergence, I present practical examples from industries like supply chain management, healthcare services, and finance. Furthermore, this research also encompasses themes such as interoperability, among systems standardization measures, edge computing applications, and privacy-oriented machine learning approaches.

Keywords: Blockchain, MQTT, Machine Learning, Internet of Things.

1. Introduction

Recent advancements in emerging technologies have catalyzed significant transformations across diverse industries, providing unprecedented opportunities for improving efficiency, security, and decision-making processes. Blockchain technology, MQTT and ML are central to this technological revolution. Each of these technologies serves as a foundational pillar, collectively reshaping information exchange dynamics, particularly within the rapidly evolving landscape of the IoT. This survey explores the convergence of these technologies, analyzing their synergistic potential and critical role in addressing contemporary challenges IoT ecosystems face.

The primary objective of this survey is to thoroughly investigate the intersections of blockchain, MQTT, and machine learning. I aim to highlight their complementary characteristics, which are essential for navigating the complexities inherent in modern IoT environments. Specifically, this exploration seeks to reveal the integration's profound impact on enhancing data security, achieving scalability, and enabling intelligent decision-making, thereby driving the progression of interconnected IoT systems.

Blockchain technology is recognized as a decentralized and immutable digital ledger, underpinning cryptocurrencies such as Bitcoin and Ethereum. Utilizing robust cryptographic algorithms, blockchain ensures transparency, security, and resistance to data manipulation, creating a trustworthy platform for secure data recording and exchange. The decentralized architecture eliminates the need for centralized authorities, fostering a peer-to-peer network model anchored by consensus mechanisms responsible for transaction validation and maintaining ledger integrity. Moreover, smart contracts enhance blockchain's capabilities by automating and executing predefined, programmable agreements, significantly streamlining processes and ensuring compliance with specified conditions [1].

In contrast, MQTT emerges as a lightweight and efficient messaging protocol specifically designed for IoT devices, characterized by their limited computational resources and constrained bandwidth capabilities. MQTT facilitates real-time data transmission, enabling seamless and efficient communication among interconnected IoT devices. MQTT devices publish messages to a central broker by employing a publish-subscribe model, disseminating relevant information to devices subscribed to specific topics. This model positions MQTT as an essential technology for scalable, responsive IoT ecosystems, effectively optimizing bandwidth utilization and power consumption [2].

Machine learning, a pivotal subset of artificial intelligence (AI), allows systems to detect patterns within data and make autonomous, informed decisions. Machine learning methodologies, including supervised, unsupervised, and reinforcement learning, support various applications such as image recognition, natural language processing, speech recognition, and predictive analytics. Integrating machine learning into IoT environments significantly enhances data-driven analytics and predictive capabilities, improving system efficiency, accuracy, and responsiveness [3].

The fusion of blockchain, MQTT, and machine learning technologies represents a potent combination capable of addressing core challenges within IoT ecosystems, including security vulnerabilities, data privacy concerns, and robust and scalable communication infrastructures. This triad substantially strengthens IoT environments, creating new avenues for innovation across multiple sectors such as healthcare, supply chain management, energy, and transportation.

This survey seeks to contribute to the existing body of knowledge by thoroughly analyzing state-of-the-art research, identifying critical research gaps, and presenting an extensive overview of the opportunities and challenges associated with leveraging blockchain, MQTT, and machine learning within IoT contexts. By doing so, I aim to stimulate further research efforts and inspire innovative solutions that can advance this interdisciplinary domain.

The subsequent sections of this paper are structured as follows: First, foundational concepts of blockchain, MQTT, and machine learning will be detailed comprehensively. Then, I will examine real-world applications and case studies, followed by insightful discussions on potential future trends. Ultimately, readers will gain a comprehensive understanding of the transformative capabilities of integrating these three technologies, setting the foundation for pioneering innovations and shaping the future trajectory of IoT development.

2. Related Work

This section aims to comprehensively review and analyze existing research on integrating blockchain, MQTT, and machine learning. Focusing on their convergence in IoT environments, I explore their potential to enhance data security, real-time communication, and data-driven decision-making. I summarize methodologies, key findings, and contributions through a structured presentation of related works, identifying trends, gaps, and challenges. This analysis sets the groundwork for deeper exploration in subsequent sections, aiming to equip readers with insights into this transformative interdisciplinary field.

In the education sector, this research [4] delves into integrating ML and blockchain technologies to address forgery issues and enhance efficiency[4]. The paper highlights the prevalence of academic record forgery and its consequences, emphasizing the need for a robust system to verify document authenticity. The proposed solution combines ML and blockchain, utilizing digitization, ML-based verification, secure blockchain storage, and authentication mechanisms. This integration enhances education sector security, simplifies verification, and promotes transparent record-keeping.

This paper [5] acknowledges the interest in combining ML and blockchain to enhance smart applications by examining the integration of ML techniques into blockchain-based smart applications. Challenges such as data privacy, compatibility with consensus mechanisms, and interoperability are identified. Strategies are suggested, including data management, federated learning for privacy, scalability methods, consensus design, and standardization efforts. The paper emphasizes interdisciplinary collaboration to harness the potential of ML and blockchain in smart applications.

An illustration of the ML threat model for IoT is presented in Figure 1. Within IoT security and privacy, this study [5] explores the application of ML and blockchain. Addressing threats such as data breaches and unauthorized access, the authors propose combining ML's anomaly detection and blockchain's immutability. The paper outlines countermeasures involving authentication, ML intrusion detection, data integrity through blockchain, and secure updates. Challenges such as scalability and collaboration are also discussed. This illustration visually represents the vulnerability of the ML model at various stages within the IoT environment.

Within this study [6], integrating blockchain and machine learning in IoT applications for advanced networks like 5G and beyond is meticulously investigated. The paper underscores the critical significance of merging these cutting-edge technologies to effectively tackle the intricate challenges encompassing data analytics, security, and privacy within the context of IoT. Delving into the intricacies, the exploration revolves around decentralized blockchain algorithms and machine learning techniques, with a strategic focus on their harmonious synergy across a diverse spectrum of applications.

As Figure 2 visually portrays, the integration of machine learning within the blockchain framework contributes to robust data quality validation. This visualization aptly captures the essence of the study's emphasis on leveraging advanced machine-learning techniques within the blockchain ecosystem to enhance data quality and integrity. By dissecting the potential applications and challenges arising from this symbiotic fusion, the research significantly contributes to advancing IoT ecosystems, aligning with this paper's overarching theme.

Amidst the dynamic landscape of the IoT, security and privacy concerns loom. This study [7], with its proposed dynamic access control policy, introduces a pioneering approach to address access control within IoT, leveraging the synergy of blockchain and machine learning. The dynamic access control policy harnesses the decentralized nature of blockchain while integrating reinforcement learning algorithms for adaptability. By amalgamating these cutting-edge technologies, the study offers a comprehensive solution that fortifies IoT security, adapts to emerging challenges, and safeguards sensitive data.

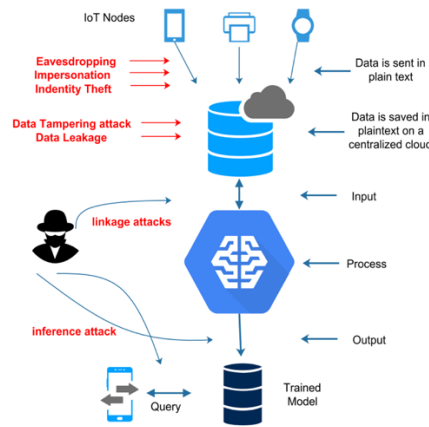


Figure 1 A depiction of the machine learning threat model specifically designed for the IoT context.

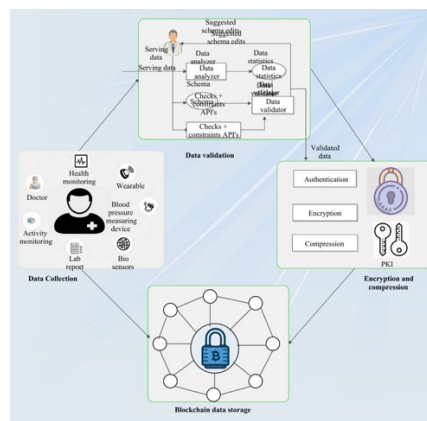


Figure 2 An illustration of ML-based blockchain data quality validation

This paper delves into advancing blockchain models within blockchain technology. It analyses existing models and their limitations. To overcome these challenges, the study introduces GraphChain, a dynamic graph data structure, and proposes a shift from competitive to parallel mining to enhance blockchain systems' efficiency. Through simulations, the paper demonstrates the potential of these innovations to optimize system capacity and performance, contributing to the evolution of blockchain technology.

Focusing on the economic significance of the Indian agricultural sector, this research in [8] highlights Contract Farming as a solution to address challenges faced by farmers. The proposed framework leverages Blockchain, IoT, and Machine Learning to create a mutually beneficial environment for corporate entities and farmers. By ensuring transparency through blockchain, real-time monitoring through IoT, and optimization through machine learning, the approach transforms Contract Farming, promoting efficiency, fair practices, and sustainable growth.

In addressing security vulnerabilities in MQTT-based IoT sensors, this paper [9] presents a novel approach by integrating blockchain, MQTT, and machine learning. The resulting blockchain-based forensic system offers a comprehensive solution encompassing evidence collection, preservation, analysis, and classification. An illustrative representation of the comparison between SMPS (Sensor-Machine Learning-Blockchain) solutions and traditional methods can be observed in Figure 3, where the system's innovative architecture is visually highlighted. By fusing the tamper-resistant nature of blockchain technology with the data analysis capabilities of machine learning, the system not only ensures the integrity of evidence through federated blockchains and employs machine learning to evaluate the severity of detected threats. This collaborative synergy significantly bolsters the security of IoT sensors, providing a dynamic and resilient approach to evidence management and safeguarding against evolving threats. This innovative integration aligns with the paper's central theme, showcasing a transformative leap in IoT sensor security.

This study [10] introduces Machine Learning Consensus-Based Lightweight Blockchain (MCLB) within the framework of energy-limited IoT contexts. MCLB uses machine learning methods to achieve consensus on data integrity, removing the conventional overhead associated with blockchain. Through experimental analysis, it has been determined that MCLB surpasses current blockchain models in both latency and efficiency. This advancement greatly enhances the administration of data on the IoT.

This research [11] focuses on ensuring data privacy and security in smart cities through the Blockchain-Enabled Privacy-

Preserving Access Control System (BPACS). Integrating blockchain, cryptographic techniques, and machine learning, BPACS encrypts and validates IoT data while safeguarding sensitive information and enabling resilient SVM and PCA algorithms. This comprehensive framework contributes to securing IoT data management within smart city contexts.

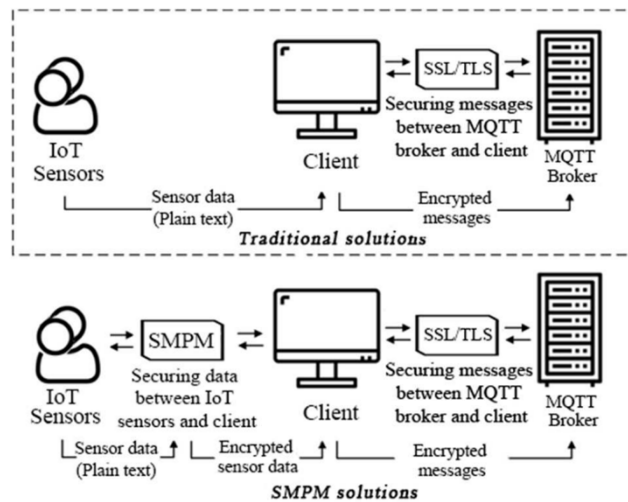


Figure 3 SMPS solutions vs. traditional solution

The traditional paradigm of employee attendance is reimaged through the convergence of IoT, machine learning, and blockchain [12]. This novel framework automates attendance processes while ensuring tamper-proof records and transparency. By integrating these technologies, the approach enhances reliability, security, and efficiency in attendance tracking.

In the rapidly evolving realm of the IoT, where seamless device interaction is paramount, safeguarding data security and transmission has emerged as a critical challenge. This study introduces a groundbreaking approach by using ML and Blockchain technologies to establish a novel Data Security Model for IoT. Referred to as the Machine Learning-based Data Security Model with Blockchain (MLDSMB) [13], this framework revolutionizes data transmission security. By leveraging Blockchain's tamper-proof data ledgering and Machine Learning's predictive capabilities, the model forms a robust defense against vulnerabilities and breaches. The architecture meticulously logs and verifies data packet transmissions through blockchain, while Machine Learning-driven insights empower proactive threat prediction and detection. Notably, MLDSMB transcends data security, enabling the seamless integration of diverse sensor types through advanced translation techniques, thus fostering rapid global IoT expansion. A comparative analysis demonstrates its exceptional data transmission security improvement, showcasing MLDSMB as an innovative solution poised to address IoT's complex security challenges.

Amidst the transformative evolution of smart cities propelled by IoT, many security and privacy challenges surface. This insightful study [14] introduces the Privacy-Preserving and Secure Framework (PPSF) that strategically harnesses blockchain, PCA, and machine learning synergies. This dynamic integration empowers the framework to ensure secure data transmission, proactive intrusion detection, and robust data privacy mechanisms within the intricate smart city landscape. Illustrated vividly in Figure 4, the proposed PPSF deployment architecture encapsulates the essence of the paper's innovative approach. This architectural representation exemplifies the intricate connections and functionalities that collectively form the backbone of the PPSF, safeguarding the foundation of IoT-driven smart cities. The research's empirical assessments further solidify its credibility by demonstrating the exceptional performance of PPSF, underscoring its efficacy as a comprehensive solution that paves the path for the sustainable growth and security of modern smart cities.

This paper [15] introduces a blockchain-based authentication protocol for enhancing the security and efficiency of Vehicular Ad hoc Networks (VANETs) on the Internet of Vehicles (IoV). Emphasizing the challenges of identity verification and communication security in highly dynamic VANETs, the authors propose a decentralized authentication service using the Ethereum blockchain. The protocol, validated for its efficiency through numerical analyses, categorizes services and IoVs to optimize communication and authentication. The lightweight design ensures minimal storage and low computational overhead, making it suitable for IoVs with limited resources. The paper contributes to addressing cyber threats in VANETs and envisions future enhancements for scalability and behavior analysis of IoVs, offering a promising solution for secure and efficient IoV communication. This study [16] presents a thorough three-tiered framework for managing data in IoT systems.

This framework combines clustering, Edge Computing (EC), and Blockchain. This study highlights the crucial issue of data management in the context of IoT, which is typically overlooked in existing research that mostly focuses on Blockchain's involvement in digital currencies, consensus algorithms, and smart contracts. The suggested framework encompasses the implementation of permissioned authentication, the development of smart contracts, the establishment of immutable block transactions, and the deployment of decentralized nodes.

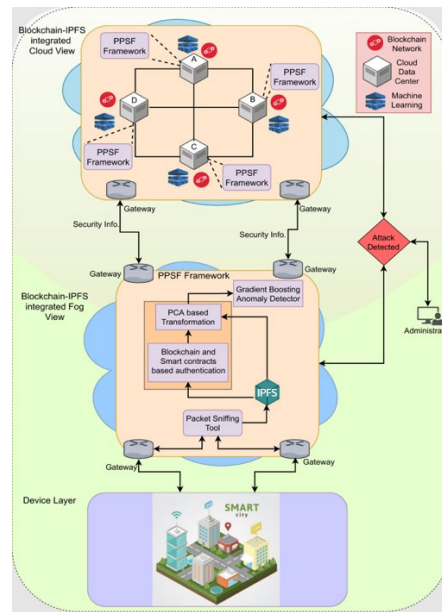


Figure 4 Proposed PPSF deployment architecture in a smart city.

The framework intends to provide a secure, tamper-resistant, and resource-optimized data management method for IoT devices by integrating clustering, blockchain, and edge computing. The study emphasizes the importance of effective data transmission, organization, and protection in the suggested paradigm, which could have consequences for improving and strengthening future IoT systems. The concluding remarks highlight the feasibility of integrating IoT with Blockchain to create secure and efficient systems, while also emphasizing the importance of additional investigation and improvement in the data management element of these linked systems.

This paper [17] explores the integration of blockchain with the IoT to address security concerns arising from the growing trend of networking furniture. The focus is on Ethereum-based smart contracts and the inherent challenges related to floating-point calculations. The proposed solution involves a calculation revamp for Ethereum-based smart contracts to enhance their computing ability and facilitate floating-point computing services. The study thoroughly verified the revamped smart contract's behavior using Remix and implemented it in a blockchain-based IoT system. The results from online tests and local deployment experiments confirm the effectiveness of the revamped smart contract. It improves computing capabilities, enables floating-point operations, and records time-sensitive data on the blockchain without data loss due to long computing times. The conclusion emphasizes the potential of this revamp to address challenges faced by small and mid-size enterprises (SMEs) in implementing smart contracts, making it a cost-effective and valuable solution for the public chain.

This paper [18] presents a blockchain-based leader election algorithm tailored for the IoT environment. In response to the increasing demand for IoT applications, the research focuses on innovative solutions for managing heterogeneous IoT networks' coordination and decision-making processes. The proposed algorithm leverages blockchain technology, with access points as full nodes participating in the election process. The outcome is selecting a leader device under the control of an access point, contributing to improved synchronization, data aggregation, and overall system efficiency. The selected leader enhances decision-making within the network and can function as an aggregator or data aggregator node. The blockchain ensures the security and integrity of the leader election process. The simulation study conducted validates the proposed protocol, demonstrating its correctness. The algorithm's efficiency is highlighted by its time complexity of $O(k*n)$ and message complexity of $O(g*n)$. The paper introduces a secure and efficient leader election mechanism for IoT networks.

This study [19] investigates the potential for revealing the character of nodes within a blockchain, focusing on the widely used cryptocurrency, Bitcoin. By releasing and labelling a dataset of almost 9,000 Bitcoin addresses, representing various roles like miners or exchanges, the research explores whether the behaviour of nodes can be deduced through features derived from transaction histories. Applying supervised learning algorithms to this dataset yields compelling results, with F-scores surpassing 95% in the most effective algorithms. The findings underscore the difficulty of concealing a node's role in a blockchain-based network and emphasize the need for meticulous design decisions in creating trustworthy blockchain systems to maintain the intended level of participant anonymity. Future research avenues include extending the approach to non-cryptocurrency blockchains, exploring collective classification techniques, identifying additional address classes, and incorporating network measures to enhance feature sets. The public release of the labelled dataset encourages further exploration and comparison by researchers in this domain.

This paper [20] presents RASSIFAB, a Firmware Over The Air (FOTA) modification technique for smart inverters (SIs) in the expanding domestic solar market. This system aims to update the firmware of smart inverters wirelessly. IoT-enabled

smart inverters introduce automation to the periphery of the energy system, but this also brings about heightened security vulnerabilities. The suggested approach employs blockchain technology to guarantee robust, verifiable, and protected firmware updates for these devices. RASSIFAB was created to facilitate the implementation of widespread Distributed Energy Resources (DERs) with diverse System Integrators (SIs), by utilizing network segmentation and blockchain sharding. The method was executed on a blockchain test network, showcasing its functionality and performance. A security assessment evaluated its resilience against attacks, demonstrating that RASSIFAB is effective and sturdy. The system guarantees secure and genuine firmware modifications, distinguishing it from current methods, even when dealing with untrustworthy individuals.

The confluence of AI, Blockchain, and IoT has the potential to bring about significant transformation in various industries. Innovative systems are produced by combining IoT's network of sensor-equipped physical devices with Blockchain's secure and decentralized ledger and AI's intelligent decision-making capabilities. This connection enables the immediate monitoring of the supply chain, the elimination of fraudulent activities, and the enhancement of efficiency. Healthcare enables the secure transmission of data and enhances diagnostic accuracy, while smart cities see improved efficiency in their urban infrastructure. Notwithstanding these prospects, stakeholders must appropriately address ethical concerns, including potential unemployment and data security, by adopting a balanced implementation strategy that considers the benefits and difficulties of this influential integration [21].

In the context of Industrial Era 4.0, IoT has become a pivotal technology, finding applications in various sectors, including agriculture. The deployment of IoT facilitates the transmission of sensor data, typically stored in databases. However, as IoT networks expand, data security and integrity challenges emerge. This study addresses these issues by proposing the implementation of blockchain technology in IoT sensor data, focusing on real-time irrigation data sensors. Utilizing the proof-of-work consensus, the Ethereum blockchain enhances data integrity and mitigates problems like data manipulation. Experimental results demonstrate the efficacy of this approach, showcasing that Ethereum-based blockchain ensures the integrity of irrigation sensor data, providing a secure and tamper-proof storage solution. Looking ahead, future work could explore the integration of machine learning to optimize the management of irrigation data further [22].

This paper [23] delves into developing a system for storing Internet of Things (IoT) data in a decentralized network, utilizing blockchain technology and smart contracts. The Ethereum blockchain manages transactions through smart contracts, while IPFS (InterPlanetary File System) is the storage solution.

The implementation involves using Solidity language for smart contract development, NodeJS for simulating IoT devices, and the MQTT protocol for data transport. The tests demonstrate this solution's advantages over direct storage in the Ethereum blockchain. The study concludes that this combination of technologies can be a valuable asset in meeting the data consumption needs of contemporary society. Future work is proposed to enhance the MQTT modules, explore using private blockchains to reduce transaction fees, and establish an IPFS cluster for greater control over data and network traffic.

This paper [24] presents the notion of Chained Distributed Machine Learning (C-DistriM) as a solution to address the difficulties related to data quality, accessibility, and transparency in healthcare AI, specifically in the context of multicentric medical imaging. The study recognizes that the use of AI in healthcare is contingent upon the availability of data of superior quality. However, legal and ethical limitations impede sharing clinically significant research data. C-DistriM is introduced as an innovative method that merges sequential distributed learning with a platform based on blockchain technology to tackle these problems. The hypothesis posits that C-DistriM has the potential to yield comparable outcomes to a conventional centralized strategy, while simultaneously providing enhanced transparency and confidence in the process of data analysis. The research showcases the viability of C-DistriM by utilizing the NSCLC-Radiomics open data to forecast the survival rate of lung cancer. The findings suggest that C-DistriM performs similarly to the centralized strategy across different scenarios. The blockchain architecture is advantageous for tracking the provenance of data and monitoring the training process for potential problems such as model degradation and dishonest behaviors.

Incorporating blockchain and distributed learning in C-DistriM is regarded as a proof-of-concept aimed at augmenting transparency, trust, and expediting the implementation of AI in multicentric studies. The conclusion highlights the practicality of the suggested methodology and its ability to promote worldwide cooperation in providing strong AI based on comprehensive datasets.

This paper [25] presents a comprehensive bibliometric analysis of blockchain and ML technology integration, covering 700 manuscripts from 2017 to 2022. Notably, the study highlights a surge in interest post-2017 and identifies influential journals, articles, and global contributors. The shift from Western Asian to East Asian research efforts is observed. The analysis incorporates co-citation and cluster approaches, revealing emerging trends and hotspots. Acknowledging limitations, the study suggests broader database exploration and alternative tools for future research. Despite limitations, this paper provides a foundational understanding and guides future research in the dynamic intersection of blockchain and ML.

This study [26] presents an innovative strategy to address financial fraud in e-commerce by integrating blockchain, smart contracts, and machine intelligence. The idea prioritizes inter-organizational collaboration while also resolving data privacy issues. The blockchain ensures the confidentiality of data, while a smart contract automates the process, enabling gradual upgrades to a machine learning model by utilizing shared data from interconnected organizations. A dynamic incentive

mechanism benefits organizations based on the complexity of model updates, promoting active involvement. The experimental results demonstrate a significant improvement in testing accuracy, Fbeta scores, and a notable decrease in the false-negative rate achieved through incremental learning. The study highlights the effectiveness of the blockchain network across different levels of difficulty and data volumes, providing a universal solution that can be used in sectors that prioritize data privacy and security. Future research aims to provide adaptable solutions that can handle continuous data streams in a class-specific manner.

This article [27] explores the security obstacles linked to smart contracts in IoT applications based on Blockchain technology, emphasizing possible hazards such as monetary losses and unauthorized disclosure of data. The article presents a new method called tree-based machine learning vulnerability detection (TMLVD) to examine smart contracts for flaws. TMLVD uses abstract syntax trees (AST) to generate intermediate representations of smart contracts, which are input into a tree-based training network to construct a predictive model. The methodology is highly efficient and efficacious in identifying vulnerabilities and providing prompt and precise outcomes, as verified through experiments conducted on Ethereum smart contracts. TMLVD distinguishes itself by targeting the drawbacks of current approaches and demonstrating enhanced detection speed and accuracy capabilities.

The primary objective of this study [28] is to exploit social media platforms for disaster and emergency response by employing automated event detection and information dissemination. The system incorporates cutting-edge Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) techniques to extract up-to-the-minute content about emergency events, hence augmenting the capacity of authorities to respond swiftly. Utilizing a blockchain architecture guarantees the verification of trust for identified events and eliminates the need for a single governing entity, enhancing system security and transparency. The primary objective of the integrated system is to enhance the precision of information exchanged on social media during disasters, therefore facilitating relief activities with more efficacy. The pipeline encompasses event detection, classification, content mapping, clustering, and trust verification, providing a comprehensive methodology for crisis management. The results demonstrate the system's proficiency in identifying pertinent subjects, evaluating methodologies, forecasting, and acquiring knowledge from modules to improve overall effectiveness.

In the contemporary era of rapid digitization and technological advancements, ML algorithms are pivotal across diverse sectors, including healthcare, IoT, engineering, and finance. However, the reliability of these algorithms hinges on the integrity of their training datasets, making them susceptible to potential tampering and bias. This article [29] proposes a blockchain-based solution aimed at fortifying the security of datasets generated from IoT devices, specifically in the context of e-health applications. The envisioned blockchain approach leverages a private cloud infrastructure to address vulnerabilities in training datasets. To assess its effectiveness, I have implemented a system empowering the dataset owner to secure their data proactively. In conclusion, future considerations involve extending the proposed blockchain solution to ensure consensus among higher officials in large-scale scenarios, accompanied by a feasibility analysis of various consensus mechanisms. Additionally, exploring decentralized storage solutions like the InterPlanetary File System (IPFS) or SWARM could offer enhanced dataset security, marking a crucial stride towards the decentralized landscape envisioned in Web 3.0.

Smart cities are at the forefront of the fast-evolving technology landscape, utilizing IoT and blockchain technologies to improve the quality of life. This article [30] presents the concept of smart cities based on the IoT and discusses the difficulties related to security and transparency in systems that include numerous parties. It proposes the use of blockchain technology as a solution to these obstacles. Nevertheless, conventional transaction processing methods relying on fees or a first-come, first-served approach can result in delays during emergencies, endangering lives. To tackle this issue, the suggested system integrates transaction prioritization, which is determined by the urgency of the information, along with a technique that creates blocks dynamically. The primary emphasis lies on a consortium blockchain that members from diverse organizations uphold to enhance efficiency. The leader election procedure in a consortium blockchain is vital for the fair prioritization of transactions. Thus, the consensus protocol incorporates a machine-learning (ML) method to facilitate efficient leader election and a dynamic block construction technique. Furthermore, a verification approach based on peer prediction is employed to guarantee the integrity of leader behaviour. The suggested approach is supported by security assessments and simulation experiments, which showcase its resilience, precision, and effectiveness. The article introduces a new machine learning-based blockchain consensus protocol for IoT-based smart cities. The protocol's efficiency is demonstrated through extensive simulations and analysis.

This work [31] investigates the convergence of blockchain technology and wireless networks, aiming to harness both advantages to establish a robust and effective framework. The accepted limits of blockchain, including expense and complexity, have resulted in a division between permissioned and permissionless blockchains.

Permissionless blockchains require significant computational resources to achieve consensus, whereas permissioned blockchains prioritize energy efficiency at the expense of decentralization. To strike a balance and address these concerns, the study suggests a new system that utilizes machine learning, specifically reinforcement learning, to autonomously acquire knowledge about the trust level of users in a public blockchain network. This trust level dictates their privileges to access a private blockchain network. This study emphasizes the potential advantages of utilizing reinforcement learning assisted blockchain technology to facilitate reliable autonomous operations and decision-making in wireless networks. The proposed architecture showcases a compelling equilibrium between the benefits of permissioned and permissionless blockchain

networks through a case study employing a blockchain-based unmanned aerial vehicle (UAV) in IoT networks. The paper highlights the significance of comprehending the basic principles of blockchain technology, evaluating its advantages and constraints, and implementing inventive approaches, such as machine learning, to augment its capabilities in particular scenarios, such as wireless communication networks.

This article [32] presents a new framework that integrates blockchain and Intel Software Guard Extension (SGX)-based trusted execution environment (TEE) to guarantee secure aggregation of local models within the Industrial Internet-of-Things (IIoTs) setting. The framework is specifically developed to mitigate the risk of tampering with local models in federated learning (FL), which refers to the situation where a global model obtained from tampered local models may result in mistakes. The suggested approach incorporates a blockchain network to enable secure model aggregation. Each blockchain node has an SGX-enabled processor responsible for securely executing federated learning-based aggregation activities and building a global model. The blockchain nodes have a vital function in validating the genuineness and soundness of the consolidated model via a consensus method. Subsequently, the validated model is securely recorded on the distributed ledger to prevent unauthorized alterations.

The framework's performance was assessed by conducting experiments using several Convolutional Neural Network (CNN) models and datasets. The results showed that the processing time was similar to the original FL model, with a slight reduction in accuracy. The proposed approach provides a reliable solution for combining local models in a federated learning environment in the context of IoT. Future work aims to improve the consensus mechanism for practical implementation and expand support for diverse tasks in blockchain-based federated learning with secure aggregation using TEE technology.

This article [33] introduces a new method for using big data to drive cognitive computing in the context of Industry 4.0. It utilizes a decentralized methodology called D2C (Decentralized Cognitive Computing). The fusion of federated learning and blockchain seeks to tackle multiple issues in this field, such as data privacy, efficiency, and safeguarding against poisoning assaults. Federated learning is utilized to address the issue of data silos by guaranteeing privacy preservation and efficient computation, while blockchain provides an incentive mechanism, total decentralization, and resilience against attacks. Utilizing blockchain in federated learning facilitates rapid convergence by implementing sophisticated verification mechanisms and member selection processes. The comprehensive assessment of the D2C platform showcases its efficacy compared to current designs and models in the domain of smart manufacturing for Industry 4.0. The article concludes by emphasizing the enhanced computational processing efficiency attained through the D2C paradigm and outlining future research plans, such as optimizing trade-offs between performance indexes and creating a tailored reward system to incentivize the involvement of public devices in high-performing industries.

This article [34] presents a complete methodology for optimizing resources, such as caching, computing, and security, in the context of delay-tolerant data in Machine-to-Machine (M2M) communications networks.

The suggested approach utilizes edge computing and blockchain technologies to deploy a dueling deep Q-network (DQN) for making dynamic decisions related to cache servers, compute servers, and blockchain systems. The goal is to optimize system incentives by improving data processing efficiency, minimizing network expenses, and enhancing data interaction security.

The simulation results illustrate the effectiveness of the proposed framework, highlighting substantial enhancements in system rewards compared to current systems. The suggested scheme's stability is intact, and forthcoming research will investigate further aspects, such as incorporating smart cities with energy-efficient M2M communications and blockchain systems into the proposed framework.

This study [35] introduces a new method called Blockchain Assisted Data Edge Verification with Consensus Algorithm for Machine Learning (BDEV-CAML) to enhance defect detection in the IoT setting. The technique combines blockchain, IoT, and ML to improve the IoT network's reliability, effectiveness, and security. Within the blockchain component, IoT devices, equipped with decentralized decision-making abilities, establish agreement on the effectiveness of transactions occurring within a block. The fault detection process utilizes the deep directional gated recurrent unit (DBiGRU) model, and the African vulture optimization algorithm (AVOA) is applied to optimize the hyperparameters, hence improving the rate of problem detection.

The experimental findings indicate that BDEV-CAML outperforms previous models, obtaining a remarkable maximum accuracy of 99.6%. Further research could investigate the use of hybrid deep learning models to improve the performance of BDEV-CAML. Additionally, it is recommended that its application be extended to real-time fault detection in IoT contexts.

This article [36] presents a Collective Q-learning (CQL) approach that utilizes blockchain technology to tackle the difficulties of combining ML with the IoT. The suggested approach entails the utilization of lightweight IoT nodes to train specific segments of learning layers. Blockchain technology facilitates the sharing of verifiable and enduring learning outcomes.

The Proof-of-Work (PoW) consensus protocol has been improved to incorporate Proof-of-Learning (PoL), in which the IoT node that achieves the lowest reduction percentage of the learning loss function is declared the winner. The CQL methodology addresses a resource allocation challenge in IoT, specifically in the context of networking integrated cloud-edge-end systems. The experimental findings demonstrate the exceptional performance of the CQL strategy. Future work

will focus on analysing the incentive mechanism of PoL to improve the overall generalization of the suggested strategy.

This paper [37] investigates the utilization of ML in blockchain-based smart applications to bolster security measures against threats. It emphasizes the importance of machine learning in analyzing secure data on the blockchain, specifically addressing concerns such as majority attacks and double-spending. The paper explores machine learning techniques such as Support Vector Machines, clustering, bagging, Convolutional Neural Network (CNN), and long short-term memory (LSTM). These techniques are specifically examined in relation to enhancing the security of blockchain networks. The report also examines ML and blockchain technology utilization in advanced fields such as Unmanned Aerial Vehicle (UAV), Smart Grid (SG), healthcare, and smart cities. The study delves into forthcoming research problems and potential opportunities, encompassing subjects such as the accessibility of infrastructure, the ability of quantum systems to withstand disruptions, and concerns related to privacy. The research finishes by presenting a case study on an energy trading system, confirming the ML-BT design's efficiency.

This paper [38] presents a solution to the issue of gradient leaking in Federated Learning (FL) by utilizing the Swarm Learning (SL) framework, which is built on blockchain technology. The gradients are distributed among the collaborative nodes in the federated learning (FL) context. However, introducing perturbations to these gradients to protect privacy can result in an issue known as gradient leaking. The suggested self-learning (SL) approach entails the distribution of the initial gradients across authorized training nodes through a secure communication strategy based on blockchain technology. The work showcases the efficacy of this strategy by employing widely recognized benchmark datasets (CIFAR10 and MNIST) and conducting a comparative analysis against established methodologies. The findings demonstrate that the supervised learning (SL) technique effectively reduces the issue of gradient leaking and attains high accuracy compared to other federated learning (FL) approaches. The report suggests that future research should investigate more effective averaging methods while preserving privacy and transforming data for collaborative supervised learning training.

This paper [39] presents a system that combines machine learning and introduces a system that integrates machine learning and blockchain technology to detect waste objects/products and provide suggestions for Do-It-Yourself (DIY) projects for their reuse or recycling.

The system employs a Deep Neural Network (DNN) utilizing the ResNet50 architecture to perform object recognition, attaining a training accuracy of 94%. Blockchain documents transactions in a communal ledger to enhance verifiability and facilitate better decision-making. Smart contracts on the Hyperledger Fabric (HF) blockchain platform verify suggested do-it-yourself (DIY) concepts. The online platform utilizes Flask, while DIY ideas are retrieved using a Python web scraping application. The study uses blockchain technology to assess smart contracts' latencies and throughput performances. Future endeavors encompass augmenting the dataset magnitude, scrutinizing the inscriptions and symbols on discarded items, and amalgamating the program with social networking platforms to enable users to disseminate their "Green Profiles" and foster greater reuse. The primary objective is to establish a worldwide network linking local government bodies, recycling plants, and thrift stores to facilitate the accessibility of recyclable garbage and encourage the adoption of a circular economy.

This paper [40] introduces a privacy-preserving distributed machine learning (DML) model for a permissioned blockchain. The main objective is to address privacy, security, and performance concerns. The authors suggest utilizing a differentially private stochastic gradient descent technique and an error-based aggregation mechanism as fundamental components. The purpose of the model is to handle a range of differentially private learning algorithms. The error-based aggregation method safeguards against assaults from adversarial nodes that aim to undermine the accuracy of DML models. The experimental findings indicate that the suggested paradigm displays robustness against malicious attacks, especially in a setting where differential privacy is maintained. The model exhibits a low level of computational complexity and transaction latency, which improves its usefulness. Future tasks involve implementing and modularizing the suggested paradigm, enabling control through chaincode functions, and applying it to the most recent iteration of Hyperledger Fabric.

This paper [41] presents a distributed computing infrastructure for implementing the L-BFGS optimization algorithm using the variance reduction method. The objective is to expedite the training procedure of machine learning models on blockchain by tackling issues associated with sluggish convergence and substantial requirements on computational and memory resources. The suggested framework is lightweight, resulting in minimal additional expenses and facilitating parallelization to enhance the efficiency of model training. The studies conducted on diverse datasets consistently reveal that the suggested computing framework effectively speeds up the training process, regardless of whether it is in local or distributed mode. The work is characterized by keywords such as machine learning and optimization algorithms.

In conclusion, the examined papers collectively acknowledge the intricate tapestry woven by the convergence of blockchain technology, MQTT protocol, and machine learning across various domains such as education, smart applications, IoT security, and beyond. Each paper contributes a distinct vantage point, shedding light on the multifaceted benefits, intricate challenges, and prospective solutions from harnessing this amalgamation of technologies. The insights from these studies illuminate the potential for augmented operational efficiency, fortified data security, and informed decision-making, signifying a significant stride toward advancing this transformative interdisciplinary realm. These seminal contributions collectively carve a path for further scholarly exploration and pioneering advancements, ushering in a new era of innovation at the intersection of blockchain, MQTT, and machine learning.

3. Blockchain Technology

Blockchain technology has emerged as a transformative force, redefining how I approach data integrity and transaction validation in decentralized systems. Fundamentally, a blockchain is a distributed ledger, characterized by its immutable and chronological nature, which is maintained across a network of nodes. This decentralization is key, eliminating the need for central authorities and relying instead on consensus mechanisms to validate transactions. This ensures trust and transparency within the network, as depicted in Figure 5 [1].

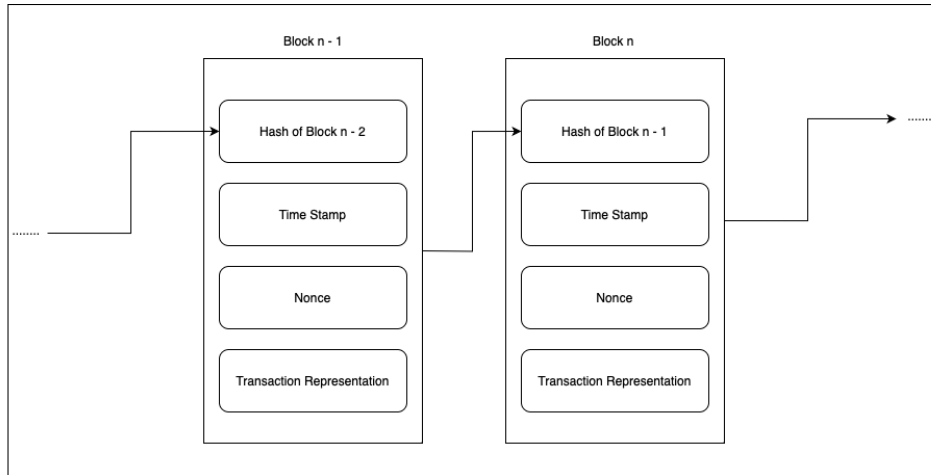


Figure 5 Blockchain Structure.

Figure 5 illustrates that each blockchain block includes a cryptographic hash of the preceding block, a timestamp, and the transaction data. The hash function acts as a cryptographic seal, ensuring the integrity of the block's contents and establishing a permanent connection to its previous block, resulting in an immutable sequence inside the chain. If any data within a block is modified, it would disrupt this cryptographic chain, indicating a breach of integrity that the network can promptly identify. The blockchain serves as a strong defense against data tampering and unauthorized changes, making it well-suited for applications that demand a high level of security, such as financial systems, supply chain management, and the protection of healthcare information [42]. Smart contracts add a level of unique functionality to blockchain technology. These automated contracts are designed to execute based on built-in logic once specific circumstances are fulfilled. They enable a wide range of applications, including automated financial agreements, decentralized apps (DApps), and the tokenization of assets. Through the utilization of smart contracts, blockchain technology surpasses its basic function of data storage and transforms into a platform capable of executing intricate business logic within a trustless environment [43].

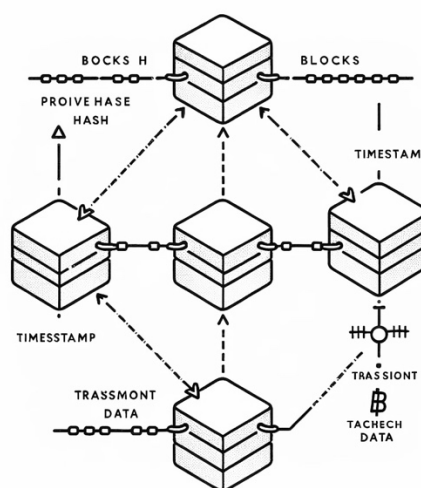


Figure 6 Simplified Blockchain Structure

Figure 6 presents a simplified view of a blockchain's structure, offering an accessible entry point for those new to the concept. It highlights the fundamental components of a block—showing the transaction data, the nonce, and the previous block's hash.

This illustration underlines the sequential nature of blockchain and the principle that each block is dependent on the hash of the block before it, emphasizing the chain's inherent security feature.

In dissecting the types of blockchains, I categorize them into public, private, and consortium blockchains, each with distinct characteristics for specific applications:

A. Public Blockchains:

Public blockchains are open, permissionless networks where anyone can participate as a node, validate transactions, and access the complete transaction history. Prominent examples include Bitcoin and Ethereum. These blockchains are pivotal in scenarios demanding transparency and openness, finding applications in cryptocurrency transactions, decentralized finance (DeFi) platforms, and other areas valuing unrestricted access [44].

B. Private Blockchains:

Contrasting their public counterparts, private blockchains operate within a confined ecosystem, accessible only to authorized participants. They offer enhanced control over governance and data privacy, making them ideal for enterprise solutions and organizations prioritizing confidential data handling. These blockchains are prevalent in sectors like supply chain management, financial services, and identity verification [45].

C. Consortium Blockchain:

Striking a balance between decentralization and control, consortium blockchains are governed by a group of pre-approved entities. While they maintain a degree of decentralization, their operations are typically overseen by a consortium, ensuring streamlined validation and governance. This type of blockchain is well-suited for industries that require collaborative efforts among various stakeholders, such as logistics, healthcare, and legal services [46].

4. Message Queuing Telemetry Transport (MQTT)

MQTT, which stands for message queuing telemetry transport, is a protocol tailored to the unique communication requirements of IoT devices, as illustrated in Figure 7, "MQTT Structure." Central to IoT ecosystems, MQTT specializes in facilitating real-time data exchange between interconnected devices, thereby playing a pivotal role in IoT communications [47].

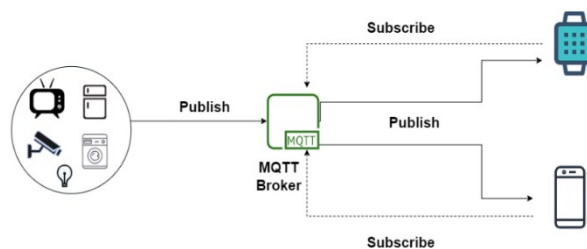


Figure 7 MQTT Structure.

Core Operation: Publish-Subscribe Model

MQTT's fundamental operation is based on a publish-subscribe messaging pattern. This model involves two primary roles:

- Publishers: These devices send messages, or "publish," to a central message broker.
- Subscribers: These devices "subscribe" to specific topics, signaling their interest in receiving messages related to those topics. The message broker serves as an intermediary, efficiently directing messages to the relevant subscribers, as detailed in Figure 7.

Key Features of MQTT:

To further understand MQTT's functionality, consider the following table summarizing its key features:

Advantages and Application:

The lightweight architecture of MQTT is perfectly suited for IoT devices that often operate under limitations of processing power, memory, and bandwidth. MQTT effectively conserves resources crucial in IoT environments by reducing protocol overhead and employing a binary message format.

Table 1 Key Features of MQTT and Their Benefits in IoT Applications

Feature	Description	Benefit in IoT Context
Lightweight Design	Minimal protocol overhead, binary message format	Ideal for resource-constrained devices; reduces data size and complexity
Real-Time Data Exchange	Low-latency communication	Supports time-sensitive applications (e.g., environmental monitoring, industrial automation)
Quality of Service (QoS) Levels	Multiple levels of message delivery assurance	Tailors message delivery reliability to application needs; balances reliability with network resources
Last Will and Testament (LWT)	Mechanism for status communication on disconnection	Ensures critical information is preserved during device failures or disconnections

Real-time data exchange capability is a cornerstone of MQTT, making it indispensable for time-sensitive IoT applications. This feature ensures prompt decision-making in scenarios like environmental monitoring and smart home systems [48].

Furthermore, MQTT's support for various Quality of Service (QoS) levels adds a layer of reliability and adaptability. These levels range from QoS 0 (at most once delivery) to QoS 2 (guaranteed single delivery), providing flexibility to cater to diverse IoT application requirements. The choice of QoS level allows for a strategic balance between reliability, bandwidth, and latency.

An additional aspect of MQTT is its support for Last Will and Testament (LWT) messages. These messages are vital for monitoring devices' status, particularly in unexpected disconnections, ensuring that essential information is not lost and maintaining the integrity of IoT operations [11].

5. Machine Learning

Machine learning is one of our most significant technological advancements, allowing systems to extract knowledge from data autonomously. ML has created a paradigm shift across various sectors by enabling enhanced data-driven decision-making, sophisticated predictive modelling, and intelligent automated pattern recognition [49]. The field of ML is broad, encompassing a range of algorithms and methods designed to interpret vast amounts of data, discover significant patterns, and make informed decisions based on these patterns.

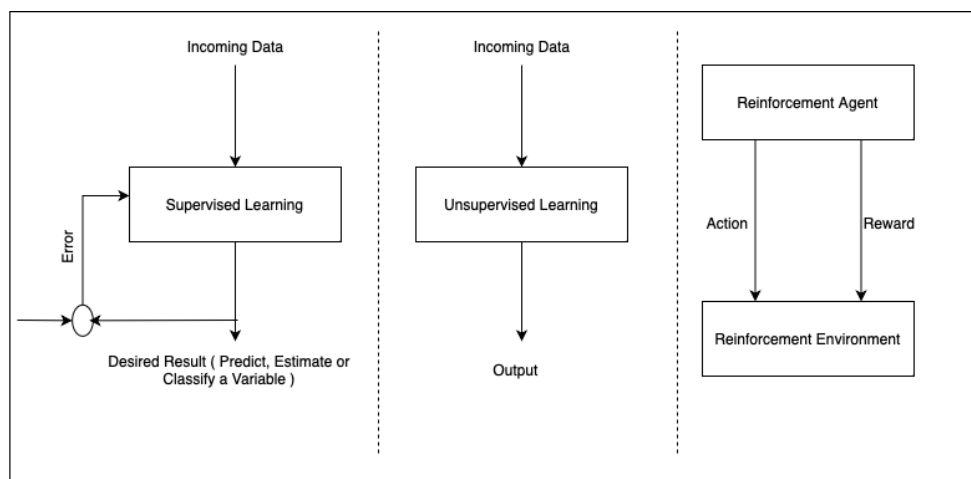


Figure 8 Supervised, Unsupervised, & Reinforcement Learning.

The Process of Machine Learning

The journey of a machine learning model begins with the **training phase**, where models learn from labelled datasets,

identifying and understanding correlations and relationships. The model builds its foundational knowledge by analyzing and interpreting the data structure in this phase. Following this is the **inference phase**, when the model applies its learned knowledge to make predictions or decisions about new, unseen data. Various machine learning techniques exist; each tailored to specific types of data and application domains [50].

Primary Categories of Machine Learning

There are three principal categories within the machine learning domain: supervised, unsupervised, and reinforcement learning. Each category approaches learning distinctly and is suited to different problems and datasets, as visualized in Figure 8.

The figure presents a schematic overview of these categories:

Supervised Learning: Here, models are fed with labelled data. They are designed to predict an output, learning from known input-output pairs to find a mapping function that generalizes well to unseen data. **Unsupervised Learning:** This approach involves models that explore unlabeled data to find inherent structures or patterns, providing insights into the underlying mechanisms of the data distribution. **Reinforcement Learning:** In this dynamic category, an agent learns from interactions with an environment, making decisions reinforced by rewards to achieve certain objectives.

Detailed Insights into Machine Learning Techniques

Supervised Learning

Supervised learning is a machine learning technique in which a model is trained with labelled data, where each input data point is paired with its corresponding proper output label. Supervised Learning aims to acquire a mapping function that reliably forecasts output labels for novel and unknown inputs. Common methods used in supervised learning encompass linear regression, logistic regression, support vector machines (SVM), decision trees, and neural networks. These algorithms have wide-ranging uses in categorization, estimation, and predicting future trends [51].

Unsupervised Learning

Unsupervised learning, in contrast, involves training the model on unlabeled data, where the ML system identifies patterns and relationships in the data without specific output labels. The primary objective of unsupervised learning is to discover underlying structures and patterns that may not be immediately evident in the data. Clustering and dimensionality reduction are two common types of unsupervised learning tasks. K-means clustering, hierarchical clustering, and principal component analysis (PCA) are popular unsupervised learning algorithms [52].

Reinforcement Learning

Reinforcement learning is a distinct form of machine learning in which an agent engages with an environment and acquires the ability to make decisions that optimize a cumulative reward. The agent is given feedback through incentives or penalties determined by its behaviors. By engaging in a process of trial and error, the agent acquires the ability to make optimal decisions to accomplish specified objectives. Reinforcement learning is utilized in robotics, game-playing, and autonomous systems. Prominent algorithms in the field of reinforcement learning encompass Q-learning and Deep Q-networks (DQNs) [53].

Table 2 Comparison of Machine Learning Categories.

Category	Description	Examples of Algorithms	Applications
Supervised Learning	Trained on labelled data with input-output pairs. Learns a mapping function for accurate predictions.	Linear Regression, Logistic Regression, Support Vector Machines (SVM), Decision Trees, Neural Networks	Classification, Regression, Time Series Forecasting
Unsupervised Learning	Trained on unlabeled data to find patterns and relationships. Discovers underlying structures and patterns in data.	K-means Clustering, Hierarchical Clustering, Principal Component Analysis (PCA)	Clustering, Dimensionality Reduction
Reinforcement Learning	The agent interacts with the environment to maximize rewards. Learns optimal decisions through trial and error.	Q-learning, Deep Q-Networks (DQNs)	Robotics, Game Playing, Autonomous Systems

Machine learning continues to evolve rapidly, with ongoing research and development pushing the boundaries of its capabilities. Techniques such as transfer learning, semi-supervised learning, and generative adversarial networks (GANs) have emerged as key areas of exploration, expanding the scope of machine learning to tackle more complex and challenging tasks [54]. To better understand the diverse approaches that machine learning encompasses, a comparison of three primary types of machine learning categories is provided in Table 2.

As illustrated in Table 2, this systematic categorization facilitates a deeper understanding of machine learning techniques and their applications across various domains. As machine learning advances, these categories provide a foundation for exploring and leveraging the capabilities of different approaches to address real-world challenges.

6. Integration of Blockchain and MQTT

The confluence of blockchain technology and MQTT is poised to significantly bolster the security and efficiency of data exchanges within the IoT domain. This integration synergizes blockchain's robust, decentralized ledger system with MQTT's streamlined messaging capabilities, presenting a formidable solution to the challenges that plague interconnected IoT infrastructures [55].

Enhancing IoT Security with Blockchain and MQTT

A prime benefit of marrying blockchain with MQTT is the substantial elevation in data exchange security within IoT networks. Blockchain's inherently distributed and tamper-proof ledger assures the immutability and transparency of data records. This assurance is critical in IoT applications where data integrity is non-negotiable, such as smart grids, healthcare monitoring, and automated supply chains. Once data is authenticated and stored on a blockchain, the likelihood of unauthorized alterations is substantially minimized, fostering a secure and reliable data exchange framework. Additionally, blockchain's decentralized topology removes the dependency on centralized data management entities, effectively diminishing potential single points of failure and augmenting the resilience of IoT systems. MQTT complements this by providing efficient, real-time communication, ensuring swift data relay between myriad IoT devices, which is vital for prompt decision-making in urgent scenarios [56].

To elucidate the nuances of blockchain and MQTT integration [57] Table 3 outlines their distinct contributions and their synergistic benefits when combined.

Table 3 Comparative Analysis of Blockchain and MQTT Integration in IoT

Feature	Blockchain Contribution	MQTT Contribution	Synergistic Benefit in IoT
Data Integrity	Immutable ledger	Efficient message delivery	Trustworthy and timely data exchange
Decentralization	No central authority	Broad device connectivity	Enhanced network resilience
Transparency	Traceable transaction history	Topic-based messaging	Clear audit trails and data flow
Security	Cryptographic security	Protocol simplicity	Robust defense against tampering
Real-time Processing	Smart contracts	Low latency	Automated and immediate actions

Overcoming Integration Challenges

While the integration brings numerous advantages, it also introduces challenges that require astute attention:

- **Data Privacy:** The public nature of many blockchains may conflict with the privacy needs of IoT applications. Solutions like private blockchains, permissioned access, and advanced cryptographic methods, such as zero-knowledge proofs or hybrid models with off-chain data handling, must be considered to preserve privacy [58].
- **Scalability:** The sheer volume of data IoT devices produce can overwhelm traditional blockchain networks. Innovations in blockchain scalability, like sharding or layer-two solutions, are vital to maintaining performance as IoT networks expand.
- **Consensus Compatibility:** Bridging MQTT's lightweight architecture with blockchain's often resource-heavy consensus algorithms is a technical hurdle. IoT-friendly consensus mechanisms like Proof-of-Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) may offer a middle ground, ensuring security without overburdening the network resources [11].

Future Prospects and Strategic Directions

As blockchain and MQTT evolve, their integration will likely become more nuanced, addressing the challenges and leveraging new developments in both fields. Research into IoT-specific blockchains, advancements in lightweight consensus protocols, and privacy preservation techniques will shape this integration's future landscape. The strategic melding of blockchain's security with MQTT's communication efficiency could redefine the standards of IoT operations, making them more secure, autonomous, and user-friendly [59].

I. Applications for Blockchain, MQTT and Machine Learning

Integrating the triumvirate of blockchain, MQTT, and machine learning has yielded a myriad of transformative applications across industries, ushering in an era of heightened data security, seamless communication, and intelligent decision-making within interconnected IoT ecosystems [60].

A. Supply Chain Management:

In the ever-evolving landscape of supply chain management, the fusion of blockchain, MQTT, and machine learning is catalyzed by the insights from recent research. This paper [61] sheds light on the profound impact of AI and blockchain on elevating supply chain performance. Blockchain, acting as a reliable framework, records data across endpoints with unprecedented frequency and granularity. AI complements this by aiding in intricate data matching, pushing the boundaries of operational effectiveness [62].

The study delves into the symbiotic relationship between blockchain and AI in supply chains, aiming to enhance operational efficiency, promote sustainable growth, and monetize data. Specifically, the exploration of blockchain in tracking financial operations within the supply chain emerges as a key focus. Additionally, the study unveils the role of AI in supply chain management, underlining its contribution to the orchestration of seamless operations.

Building upon this, another insightful contribution is drawn from this paper [63], while blockchain initially found its roots in finance, its expanding influence in the retail industry becomes evident. The paper emphasizes the transformative potential of blockchain in modernizing retail supply chains, addressing the challenges of customer confidence and loyalty.

The IEEE Standard for the Use of Blockchain in Supply Chain Finance provides a structured framework, defining essential roles and procedural steps for blockchain-driven supply chain finance implementations. This standard delineates the core elements of registration, asset issuance, transfer, financing, clearing, settlement, and tracing within the supply chain. Furthermore, it outlines the technical requirements for the business system and the blockchain platform, setting a foundational standard for industry-wide adoption. The integration of blockchain with Enterprise Resource Planning (ERP) systems for enhanced supply chain performance is explored in-depth in this paper [64]. The literature study reveals how blockchain, with its proven track record in areas like finance, can be strategically amalgamated with ERP systems to address supply chain challenges and significantly improve overall performance [65]. The study delves into the transformative potential of Blockchain of Things (BoT) and IoT in mitigating the challenges posed by globalization in supply chain management. The study, based on insights from 140 IT experts and managers, demonstrates how the integration of BoT and IoT fosters transparency, efficiency, security, and traceability, offering a foundation for faster decision-making and improved collaboration.

Finally, this paper [66] suggests blockchain as a compelling solution to the challenges in information visibility and physical flow traceability within the supply chain. The paper underscores the potential of blockchain to enhance supply chain sustainability, trust, traceability, and transparency, using the shipping industry as a poignant example. In essence, these studies collectively amplify the narrative of integrating blockchain, MQTT, and machine learning in supply chain management, offering profound insights into the nuances, challenges, and transformative potential of this interdisciplinary synergy.

B. Healthcare

The revolutionary synergy between blockchain and machine learning in healthcare is vividly demonstrated in this paper [67]. Here, the proposed architecture introduces a novel approach by incorporating Federated Learning to bolster patient data privacy. The model allows for local data training in hospitals, maintains a high level of privacy, and securely composes Smart Contracts to upload locally trained models to the Public Healthcare System. Notably, the integration of sidechains effectively addresses blockchain bottlenecks, significantly enhancing processing speed and transaction throughput, thereby optimizing overall healthcare system performance.

In the realm of healthcare evolution, this paper [68] explores the diversification of blockchain beyond finance. The blockchain management system undergoes automation using reinforcement learning, marking a significant shift into diverse domains. This innovative fusion showcases the efficiency of agents trained through reinforcement learning in executing healthcare system blockchain management tasks, underscoring the broader applications of blockchain and artificial intelligence.

The integration of machine learning and blockchain takes center stage in [69]. This paper tackles the intricacies of healthcare data management by leveraging machine learning, particularly Convolutional Neural Networks (CNN), for automatic diagnosis. With its consensus protocol, Blockchain ensures data authenticity and transaction security, placing the patient at

the core of an advanced healthcare system with improved administration.

Pioneering the introduction of blockchain technology in healthcare, this paper [70] emphasizes the critical role of blockchain in securing patient health records. The decentralized blockchain database provides extreme privacy, and machine learning algorithms, particularly the Naive Bayes classifier, are harnessed for disease prediction. The proposed system envisions improved security, reduced costs, and decentralized smart healthcare systems, showcasing the transformative potential of integrating emerging technologies.

The innovative study [71] presents a strategy that utilizes blockchain and AI technologies to address privacy concerns and the issue of fragmented medical data. Blockchain guarantees data access protection, while AI-based federated learning is implemented to construct strong models in a live and practical setting. This innovative method addresses difficulties in developing universal prediction models and emphasizes the crucial role of blockchain and AI in improving practical healthcare applications.

C. Energy Management

In the quest for sustainable and decentralized energy management, this paper [72] outlines a visionary approach. With the exponential growth in renewable energy generation, the proposed model integrates traditional and sustainable sources into an efficient energy management system. Blockchain technology was introduced to establish a secure, immutable, and trustless power distribution system, leveraging the decentralized nature of smart grids. The model facilitates peer-to-peer energy transmission by integrating all energy sources, identifying stakeholders, generating certificates/tokens, conducting energy transactions, and incentivizing sustainable or green energy use.

Proposing a novel solution, [73] addresses the difficulties of dispersed energy resources and the IoT in Prosumer Nano-Grids (P-NGs) presents. This system, which combines distributed power flow coloring, blockchain technology, and Transactive Energy Management (TEM), offers secure, transparent, reliable, and efficient energy management and transaction capabilities for P-NGs. The model guarantees the maintenance of stable voltage levels, adherence to prescribed power ratios, enhanced energy security, continuous real-time monitoring, and minimized energy wastage within the P-NG [74].

In relation to Battery Energy Storage Systems (BESS), [75] presents an advanced method for Battery Management System (BMS). The suggested system securely shares real-time data from Battery Energy Storage Systems (BESSs) using blockchain, IoT devices, and a decentralized framework. This allows for precise determination of the system's current condition, including the charge level, health, power, energy, temperature, and safety. The solution based on blockchain technology guarantees the confidentiality, clarity, verifiability, and effective supervision and management of BESSs.

This paper [76] examines the difficulties in accessing electricity in Sub-Saharan African nations. The suggested energy management system integrates a blockchain-based peer-to-peer (P2P) local energy market, specifically focusing on community-based off-grid systems. This proposal tackles the constraints of integrating isolated communities into national utility networks and guarantees an equitable mechanism for distributing quotas. The incorporation of blockchain technology enables a clear and efficient local energy marketplace, allowing for the optimal utilization of accessible energy supplies and enhancing the feasibility of off-grid solutions.

D. Finance

The combination of blockchain and machine learning is transforming portfolio management into the ever-changing field of financial applications. This study [77] presents a prototype of a portfolio management system within the decentralized Web3 environment. This system utilizes a cutting-edge machine learning-powered recommendation subsystem. It employs a distinctive account structure that mixes user-defined functions with automated asset management operations. Integrating blockchain with artificial intelligence yields a sophisticated portfolio management system that enhances efficiency and mitigates risk in asset transactions [78].

This study focuses on the crucial issue of risk and return in financial products within the context of financial globalization. The LS ODL-BFPRR utilizes machine learning and deep learning techniques to estimate return rates in the blockchain financial sector, making it an efficient tool. Using stacked bidirectional gated recurrent units (SBiGRU) in return rate categorization showcases exceptional forecasting abilities. Incorporating the Ethereum return rate as the objective and utilizing the Lion Swarm Optimization (LSO) algorithm for adjusting hyperparameters considerably augments the precision and effectiveness of return rate prediction in blockchain financial products.

This paper [79] explores the utilization of blockchain technology in the field of supply chain financing. The essay recognizes the ongoing progress in supply chain financing but highlights the drawbacks of conventional methods that lead to higher transaction costs and operational intricacies. The article examines the potential of blockchain technology to transform supply chain finance, envisioning a future where blockchain technology plays a crucial role in financial services within supply chains.

These examples represent the vast potential of integrating blockchain, MQTT, and machine learning in various industries. As research and development in this interdisciplinary domain continue to evolve, more innovative applications are expected to emerge, further propelling the transformation of IoT ecosystems and driving advancements in data-driven solutions across

diverse sectors. By harnessing the collective power of these technologies, industries can unlock new possibilities, enhance operational efficiency, and address complex challenges in an interconnected world.

7. Conclusion

This survey has provided a comprehensive examination of the integration of blockchain, Message Queuing Telemetry Transport (MQTT), and machine learning (ML) within the Internet of Things (IoT) ecosystem. The analysis has highlighted how blockchain contributes decentralization, immutability, and enhanced security; MQTT ensures lightweight and scalable communication for resource-constrained IoT devices; and ML offers predictive and adaptive intelligence for decision-making. Together, these technologies form a powerful triad that strengthens IoT applications by improving data integrity, efficiency, and resilience.

However, several critical challenges remain to be addressed before widespread adoption can be realized. Scalability is a pressing issue, as blockchain consensus mechanisms and ML computations can introduce latency and overhead in large-scale IoT deployments. Privacy also requires careful consideration, particularly in managing sensitive user or sensor data across distributed environments. Furthermore, interoperability between heterogeneous IoT devices and the seamless integration of blockchain and ML frameworks remain significant hurdles.

Future research should focus on lightweight blockchain consensus algorithms, privacy-preserving machine learning approaches (e.g., federated learning), and standardized frameworks that promote interoperability among diverse IoT platforms. A hybrid architecture combining edge computing, fog computing, and cloud resources could also balance performance and scalability. By addressing these research directions, integrating blockchain, MQTT, and ML can evolve into a foundational pillar for next-generation IoT applications, supporting secure, intelligent, and scalable ecosystems.

References

- [1] B. Bitcoin *et al.*, “Blockchain Technology,” 2015.
- [2] I. Latin and A. Transactions, “MQTT Protocol: Fundamentals, Tools and Future Directions,” 2019.
- [3] IEEE Staff, *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, 2019.
- [4] S. Bhatnagar, “Integrated Blockchain and AI Research Infrastructure for IoT Based Applications,” in *2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1140–1144. doi: 10.1109/AISC56616.2023.10085063.
- [5] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, “Semantic Similarity Metrics for Evaluating Source Code Summarization,” in *IEEE International Conference on Program Comprehension*, IEEE Computer Society, 2022, pp. 36–47. doi: 10.1145.
- [6] A. Miglani and N. Kumar, “Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review,” *Comput Commun*, vol. 178, pp. 37–63, Oct. 2021, doi: 10.1016/j.comcom.2021.07.009.
- [7] A. Outchakoucht and J. P. Leroy, “Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things,” 2017. [Online]. Available: www.ijacsa.thesai.org
- [8] S. Saxena, S. Khare, and S. Pal, “A Blockchain and Machine Learning based IoT Framework to Improve Contract Farming,” in *2021 IEEE Globecom Workshops, GC Wkshps 2021 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/GCWkshps52748.2021.9682083.
- [9] C. Wan, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, “A Blockchain Based Forensic System for IoT Sensors using MQTT Protocol,” in *2022 9th International Conference on Internet of Things, Systems, Management and Security, IOTSMS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/IOTSMS58070.2022.10062190.
- [10] A. T., S. Babu, and B. S. Manoj, “A Machine Learning Consensus Based Light-Weight Blockchain Architecture for Internet of Things,” in *2022 14th International Conference on COMMunication Systems and NETWORKS, COMSNETS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1–6. doi: 10.1109/COMSNETS53615.2022.9668487.
- [11] V. A. Athavale, A. Bansal, S. Nalajala, and S. Aurelia, “WITHDRAWN: Integration of blockchain and IoT for data storage and management,” *Mater Today Proc*, Oct. 2020, doi: 10.1016/j.matpr.2020.09.643.
- [12] A. Dixit, A. Trivedi, and W. W. Godfrey, “IoT and Machine Learning based Peer to Peer Framework for Employee Attendance System using Blockchain,” in *Proceedings - International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1088–1093. doi: 10.1109/ICAISS55157.2022.10010846.

- [13] S. C. Ch, S. Puli, K. Lakshmi Viveka, and M. V. B. T. Santhi, "Machine Learning Based Data Security Model Using Blockchain for Secure Data Transmission in IoT," in *Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESCS 2021*, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 1521–1527. doi: 10.1109/ICESCS51422.2021.9532659.
- [14] P. Kumar *et al.*, "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," *IEEE Trans Netw Sci Eng*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021, doi: 10.1109/TNSE.2021.3089435.
- [15] A. F. M. Suaib Akhter, M. Ahmed, A. F. M. Shahen Shah, A. Anwar, A. S. M. Kayes, and A. Zengin, "A blockchain-based authentication protocol for cooperative vehicular ad hoc network," *Sensors (Switzerland)*, vol. 21, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/s21041273.
- [16] D. D. Datiri and M. Li, "A Cluster enabled Blockchain-based Data management for IoT systems," in *Proceedings of the 2023 24th International Carpathian Control Conference, ICCS 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 88–92. doi: 10.1109/ICCS57093.2023.10178949.
- [17] C. Yiyang and K. Takashio, "A Floating Calculation Revamp For the Ethereum Blockchain-Based IoT Systems," in *2022 IEEE 8th World Forum on Internet of Things, WF-IoT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/WF-IoT54382.2022.10152068.
- [18] K. Kumari and M. Kumar Murmu, "A Leader Election Algorithm Using Blockchain for IoT", doi: 10.1109/AIC.2023.135.
- [19] R. Michalski, D. Dziubaltowska, and P. MacEk, "Revealing the Character of Nodes in a Blockchain with Supervised Learning," *IEEE Access*, vol. 8, pp. 109639–109647, 2020, doi: 10.1109/ACCESS.2020.3001676.
- [20] R. Akkaoui, A. Stefanov, P. Palensky, and D. H. J. Epema, "Resilient, Auditable and Secure IoT-Enabled Smart Inverter Firmware Amendments With Blockchain," *IEEE Internet Things J*, pp. 1–1, 2023, doi: 10.1109/JIOT.2023.3321954.
- [21] S. P. J, A. S, U. ranee L, T. F. A, M. S, and M. S, "Revolutionizing Industries Through IoT, Blockchain and AI Integration," in *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, IEEE, Jun. 2023, pp. 972–977. doi: 10.1109/ICPCSN58827.2023.00166.
- [22] A. Sumarudin *et al.*, "Implementation of IoT Sensored Data Integrity for Irrigation in Precision Agriculture Using Blockchain Ethereum," in *2022 5th International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 29–33. doi: 10.1109/ISRITI56927.2022.10052902.
- [23] J. P. De Brito Goncalves, G. Spelta, R. Da Silva Villaca, and R. L. Gomes, "IoT Data Storage on a Blockchain Using Smart Contracts and IPFS," in *Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 508–511. doi: 10.1109/Blockchain55522.2022.00078.
- [24] F. Zerka *et al.*, "Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM)," *IEEE Access*, vol. 8, pp. 183939–183951, 2020, doi: 10.1109/ACCESS.2020.3029445.
- [25] N. El Akrami, M. Hanine, E. S. Flores, D. G. Aray, and I. Ashraf, "Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends From Bibliometric Analysis," *IEEE Access*, vol. 11, pp. 78879–78903, 2023, doi: 10.1109/ACCESS.2023.3298371.
- [26] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach," *IEEE Access*, vol. 10, pp. 87115–87134, 2022, doi: 10.1109/ACCESS.2022.3198956.
- [27] Q. Zhou, K. Zheng, K. Zhang, L. Hou, and X. Wang, "Vulnerability Analysis of Smart Contract for Blockchain-Based IoT Applications: A Machine Learning Approach," *IEEE Internet Things J*, vol. 9, no. 24, pp. 24695–24707, Dec. 2022, doi: 10.1109/JIOT.2022.3196269.
- [28] Z. Shahbazi and Y. C. Byun, "Blockchain-Based Event Detection and Trust Verification Using Natural Language Processing and Machine Learning," *IEEE Access*, vol. 10, pp. 5790–5800, 2022, doi: 10.1109/ACCESS.2021.3139586.
- [29] T. R. Gadekallu, M. M K, S. K. S, N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 30–33, Sep. 2021, doi: 10.1109/iotm.1021.2000160.
- [30] S. V. Sanghami, J. J. Lee, and Q. Hu, "Machine-Learning-Enhanced Blockchain Consensus With Transaction

- Prioritization for Smart Cities,” *IEEE Internet Things J*, vol. 10, no. 8, pp. 6661–6672, Apr. 2023, doi: 10.1109/JIOT.2022.3175208.
- [31] A. S. Khan, X. Zhang, S. Lambotharan, G. Zheng, B. Assadhan, and L. Hanzo, “Machine Learning Aided Blockchain Assisted Framework for Wireless Networks,” *IEEE Netw*, vol. 34, no. 5, pp. 262–268, Sep. 2020, doi: 10.1109/MNET.011.1900643.
- [32] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and M. Almashor, “Blockchain-Based Federated Learning With Secure Aggregation in Trusted Execution Environment for Internet-of-Things,” *IEEE Trans Industr Inform*, vol. 19, no. 2, pp. 1703–1714, Feb. 2023, doi: 10.1109/TII.2022.3170348.
- [33] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, “A Blockchain Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks,” *IEEE Trans Industr Inform*, vol. 17, no. 4, pp. 2964–2973, Apr. 2021, doi: 10.1109/TII.2020.3007817.
- [34] M. Li, F. R. Yu, P. Si, W. Wu, and Y. Zhang, “Resource Optimization for Delay-Tolerant Data in Blockchain-Enabled IoT with Edge Computing: A Deep Reinforcement Learning Approach,” *IEEE Internet Things J*, vol. 7, no. 10, pp. 9399–9412, Oct. 2020, doi: 10.1109/JIOT.2020.3007869.
- [35] T. Vaiyapuri, K. Shankar, S. Rajendran, S. Kumar, S. Acharya, and H. Kim, “Blockchain Assisted Data Edge Verification With Consensus Algorithm for Machine Learning Assisted IoT,” *IEEE Access*, vol. 11, pp. 55370–55379, 2023, doi: 10.1109/ACCESS.2023.3280798.
- [36] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, “Networking Integrated Cloud-Edge-End in IoT: A Blockchain-Assisted Collective Q-Learning Approach,” *IEEE Internet Things J*, vol. 8, no. 16, pp. 12694–12704, Aug. 2021, doi: 10.1109/JIOT.2020.3007650.
- [37] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W. C. Hong, “Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward,” *IEEE Access*, vol. 8, pp. 474–448, 2020, doi: 10.1109/ACCESS.2019.2961372.
- [38] H. A. Madni, R. M. Umer, and G. L. Foresti, “Blockchain-Based Swarm Learning for the Mitigation of Gradient Leakage in Federated Learning,” *IEEE Access*, vol. 11, pp. 16549–16556, 2023, doi: 10.1109/ACCESS.2023.3246126.
- [39] S. Pandey *et al.*, “Do-It-Yourself Recommender System: Reusing and Recycling With Blockchain and Deep Learning,” *IEEE Access*, vol. 10, pp. 90056–90067, 2022, doi: 10.1109/ACCESS.2022.3199661.
- [40] H. Kim, S. H. Kim, J. Y. Hwang, and C. Seo, “Efficient privacy-preserving machine learning for blockchain network,” *IEEE Access*, vol. 7, pp. 136481–136495, 2019, doi: 10.1109/ACCESS.2019.2940052.
- [41] “Z. Huang, F. Liu, M. Tang, J. Qiu, Y. Peng, “A Distributed Computing Framework Based on Lightweight Variance Reduction Method to Accelerate Machine Learning Training on Blockchain,” *China Communications*, vol. 17, no. 9, pp. 77-89, Sep. 2020, doi: 10.23919/JCC.2020.09.007”.
- [42] M. Ghafourian *et al.*, “Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis,” Feb. 2023, [Online]. Available: <http://arxiv.org/abs/2302.10883>
- [43] T. Hewa, M. Ylianttila, and M. Liyanage, “Survey on blockchain based smart contracts: Applications, opportunities and challenges,” *Journal of Network and Computer Applications*, vol. 177. Academic Press, Mar. 01, 2021. doi: 10.1016/j.jnca.2020.102857.
- [44] D. Huang, C. J. Chung, Q. Dong, J. Luo, and M. Kang, “Building private blockchains over public blockchains (POP): An attribute-based access control approach,” in *Proceedings of the ACM Symposium on Applied Computing*, Association for Computing Machinery, 2019, pp. 355–363. doi: 10.1145/3297280.3297317.
- [45] T. Ncube, N. Dlodlo, and A. Terzoli, “Private Blockchain Networks: A Solution for Data Privacy,” in *2020 2nd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/IMITEC50163.2020.9334132.
- [46] O. Dib, A. Durand, K.-L. Brousmiche, E. Thea, and B. Hamida, “Consortium Blockchains: Overview, Applications and Challenges,” 2018. [Online]. Available: <http://www.iariajournals.org/telecommunications/2018>,
- [47] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, “Secure MQTT for Internet of Things (IoT),” in *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, Institute of Electrical and Electronics Engineers Inc., Sep. 2015, pp. 746–751. doi: 10.1109/CSNT.2015.16.
- [48] IEEE Systems Council and Institute of Electrical and Electronics Engineers, *ISSE 2017 : 2017 IEEE International Symposium on Systems Engineering : Vienna, Austria, October 11-13, 2017 : 2017 symposium proceedings*.

- [49] F. ARTKIN, "Applications of Artificial Intelligence in Mechanical Engineering," *European Journal of Science and Technology*, Dec. 2022, doi: 10.31590/ejosat.1224045.
- [50] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and Machine Learning for Communications and Networking Systems," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1392–1431, Apr. 2020, doi: 10.1109/COMST.2020.2975911.
- [51] A. Singh, "Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM)," 2016.
- [52] S. Naeem, A. Ali, S. Anam, and M. M. Ahmed, "An Unsupervised Machine Learning Algorithms: Comprehensive Review," *International Journal of Computing and Digital Systems*, vol. 13, no. 1, pp. 911–921, 2023, doi: 10.12785/ijcds/130172.
- [53] T. P. Lillicrap *et al.*, "Continuous control with deep reinforcement learning," Sep. 2015, [Online]. Available: <http://arxiv.org/abs/1509.02971>
- [54] A. Alzahrani and T. H. H. Aldhyani, "Artificial Intelligence Algorithms for Detecting and Classifying MQTT Protocol Internet of Things Attacks," *Electronics (Switzerland)*, vol. 11, no. 22, Nov. 2022, doi: 10.3390/electronics11223837.
- [55] M. Abdelrazig Abubakar, Z. Jaroucheh, A. Al-Dubai, and X. Liu, "Blockchain-based identity and authentication scheme for MQTT protocol," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. 2021, pp. 73–81. doi: 10.1145/3460537.3460549.
- [56] F. Buccafurri, V. De Angelis, and R. Nardone, "Securing MQTT by blockchain-based otp authentication," *Sensors (Switzerland)*, vol. 20, no. 7, Apr. 2020, doi: 10.3390/s20072002.
- [57] G. Kalele, "An In-Depth Examination of Traditional, Blockchain, and AI-Based Key-Security for The Cyber-Physical IoT Networks," *Institute of Electrical and Electronics Engineers (IEEE)*, Jul. 2023, pp. 2004–2008. doi: 10.1109/icacite57410.2023.10182722.
- [58] N. Adhikari and M. Ramkumar, "IoT and Blockchain Integration: Applications, Opportunities, and Challenges," *Network*, vol. 3, no. 1, pp. 115–141, Mar. 2023, doi: 10.3390/network3010006.
- [59] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181. Academic Press, May 01, 2021. doi: 10.1016/j.jnca.2021.103007.
- [60] S. Menon *et al.*, "Blockchain and Machine Learning Inspired Secure Smart Home Communication Network," *Sensors*, vol. 23, no. 13, Jul. 2023, doi: 10.3390/s23136132.
- [61] K. Nethravathi, A. Tiwari, D. Uike, R. Jaiswal, and K. Pant, "Applications of Artificial Intelligence and Blockchain Technology in Improved Supply Chain Financial Risk Management," in *Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 242–246. doi: 10.1109/IC3I56241.2022.10072787.
- [62] M. Alazab, S. Alhyari, A. Awajan, and A. B. Abdallah, "Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance," *Cluster Comput*, vol. 24, no. 1, pp. 83–101, Mar. 2021, doi: 10.1007/s10586-020-03200-4.
- [63] M. Hader, A. Elmhamedi, and A. Abouabdellah, "Blockchain technology in supply chain management and loyalty programs: Toward blockchain implementation in retail market," in *2020 13th International Colloquium of Logistics and Supply Chain Management, LOGISTIQUA 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/LOGISTIQUA49782.2020.9353879.
- [64] I. Lahlou and N. Motaki, "Integrating Blockchain with ERP systems for better supply chain performance," in *2022 IEEE 14th International Conference of Logistics and Supply Chain Management, LOGISTIQUA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/LOGISTIQUA55056.2022.9938086.
- [65] G. K. Singh and M. Dadhich, "Supply Chain Management Growth With the Adoption of Blockchain Technology (BoT) and Internet of Things (IoT)," *Institute of Electrical and Electronics Engineers (IEEE)*, Jul. 2023, pp. 321–325. doi: 10.1109/icacite57410.2023.10182619.
- [66] Y. Khaoua, Y. Mouzouna, J. Arif, F. Jawab, and M. Azari, "The Contribution of Blockchain Technology in the Supply Chain Management: The Shipping Industry as an Example," in *2022 IEEE 14th International Conference of Logistics and Supply Chain Management, LOGISTIQUA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/LOGISTIQUA55056.2022.9938046.
- [67] M. M. Salim, L. Park, and J. H. Park, "A Machine Learning based Scalable Blockchain architecture for a secure Healthcare system," in *International Conference on ICT Convergence*, IEEE Computer Society, 2022, pp. 2231–2234.

doi: 10.1109/ICTC55196.2022.9952962.

- [68] M. J. J. Gul, A. Paul, S. Rho, and M. Kim, "Blockchain based healthcare system with Artificial Intelligence," in *Proceedings - 2020 International Conference on Computational Science and Computational Intelligence, CSCSI 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 740–741. doi: 10.1109/CSCSI51800.2020.00138.
- [69] A. Haddad, M. H. Habaebi, M. R. Islam, and S. A. Zabidi, "Blockchain for Healthcare Medical Records Management System with Sharing Control," in *2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications, ICSIMA 2021*, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 30–34. doi: 10.1109/ICSIMA50015.2021.9526301.
- [70] Wajiha and S. R. Patil, "Implementing Blockchain Technology in Healthcare Systems utilizing Machine learning Techniques," in *2022 IEEE North Karnataka Subsection Flagship International Conference, NKCon 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/NKCon56289.2022.10126874.
- [71] Global IT Research Institute, IEEE Communications Society, and Institute of Electrical and Electronics Engineers, *The 23rd International Conference on Advanced Communications Technology: "On-Line security in Pandemic Era!" : Phoenix Park, Pyeongchang, Korea (South), (On-line Conference), Feb. 07-10, 2021 : proceeding & journal*.
- [72] J. Dargan, N. Gupta, and L. Singh, "Blockchain Based Energy Management System: A Proposed Model," in *Proceedings of International Conference on Technological Advancements and Innovations, ICTAI 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 510–514. doi: 10.1109/ICTAI53825.2021.9673233.
- [73] A. Bin Masood, S. Javaid, Y. Tan, V. Vassiliou, and M. Lestas, "A Blockchain-Based Transactive Energy Management Scheme for Nano-Grids using Power Flow Coloring," Institute of Electrical and Electronics Engineers (IEEE), Aug. 2023, pp. 187–188. doi: 10.1109/icce-taiwan58799.2023.10226681.
- [74] A. Jayavarma, Preetha, and M. G. Nair, "A secure energy trading in a smart community by integrating Blockchain and machine learning approach," *Smart Science*, 2023, doi: 10.1080/23080477.2023.2270820.
- [75] F. Mohammadi, M. Sanjari, and M. Saif, "A Real-Time Blockchain-Based State Estimation System for Battery Energy Storage Systems," in *2022 IEEE Kansas Power and Energy Conference, KPEC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/KPEC54747.2022.9814731.
- [76] I. Demidov, H. Dibaba, A. Pinomaa, S. Honkapuro, and M. Nieminen, "Energy Management System for Community-Centered Off-Grid System with a Blockchain-Based P2P Energy Market," in *International Conference on the European Energy Market, EEM*, IEEE Computer Society, 2023. doi: 10.1109/EEM58374.2023.10161848.
- [77] T. Cai, J. Wu, C. Yu, and V. Brusica, "Blockchain with Machine Learning for Financial Portfolio Management," in *ICEIEC 2023 - Proceedings of 2023 IEEE 13th International Conference on Electronics, Information and Emergency Communication*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 255–259. doi: 10.1109/ICEIEC58029.2023.10201043.
- [78] P. Sudha, J. J. Amalraj, and M. Sivakumar, "Lion Swarm Optimization with Deep Learning Driven Predictive Model on Blockchain Financial Product Return Rates," in *Proceedings of the 2023 2nd International Conference on Electronics and Renewable Systems, ICEARS 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1076–1080. doi: 10.1109/ICEARS56392.2023.10085579.
- [79] J. Chen, "Research on the Application of Blockchain Technology in Supply Chain Financial Business," in *Proceedings - 2020 2nd International Conference on Applied Machine Learning, ICAML 2020*, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 371–374. doi: 10.1109/ICAML51583.2020.00081.

Article Information Form

Acknowledgments

The authors would like to thank Sakarya University, Computer and Information Engineering Department, for their continuous support throughout this research. We also express our gratitude to the Scientific Journals Coordination Office for their guidance during the review and publication process.

Conflict of Interest Notice

The authors declare that there is no conflict of interest regarding the publication of this article.

Support/Supporting Organizations

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethical Approval

This study does not involve human participants or animals. Hence, ethical approval was not required.

Availability of data and material

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Artificial Intelligence Statement

Artificial intelligence (AI) tools were used to assist in language editing and formatting improvements during manuscript preparation. However, all intellectual content, analyses, and conclusions are the original work of the authors.

Plagiarism Statement

This article has been scanned by iThenticate™.