International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Machine Learning-based Predictive Analytics for Blockchain-enabled IoT Systems

Dr. Tripti Sharma[1], Dr. Shahanawaj Ahamad[2,*], Neeraj Gupta[3], Sivashankar P T[4], Eda Bhagyalakshmi[5], Elangovan Muniyandy[6], Ankur Gupta[7]

Submitted: 04/02/2024 **Revised**: 12/03/2024 **Accepted**: 18/03/2024

Abstract: In the realm of blockchain-enabled IoT systems, machine learning-based predictive analytics serves as a cornerstone for optimizing operations, enhancing security, and maximizing efficiency. By leveraging the wealth of data generated by IoT devices and immutably recorded on the blockchain, predictive analytics algorithms can discern patterns, detect anomalies, and forecast future events with remarkable accuracy. One key application lies in anomaly detection, where machine learning models scrutinize data to identify aberrant behavior or potential security threats in real-time, thereby fortifying the integrity of the system. Moreover, predictive maintenance emerges as a vital capability, as machine learning algorithms analyze historical data to anticipate equipment failures or maintenance needs, preempting costly downtime and prolonging device lifespan. This paper is considering research in area of machine learning for predictive analysis that are made for blockchain enabled IoT system. Paper has focused on role of ML based predictive analytics and conventional research in related area. Moreover works related to blockchain enabled IoT system and ML based predictive system are focused with their methodology, limitations, outcomes and future scope.

Keywords: *Machine learning, Blockchain, IoT, Predictive analytics*

1. Introduction

The combination of artificial intelligence (AI), machine learning (ML), predictive analytics (PA), blockchain technology, and Internet of Things (IoT) technologies gives a compelling possibility to improve data-driven decision-making across a variety of fields. On account of the exponential growth of Internet of Things devices that generate vast streams of data, as well as the inherent difficulties of ensuring data integrity, privacy, and security in decentralized environments, there is an urgent need for innovative solutions that are able to extract actionable insights from this flood of information. In response to this problem, academics and practitioners have increasingly resorted to machine learning-based predictive analytics approaches to generate value from Internet of Things (IoT) data. At the same time, they have used blockchain technology to provide trust, transparency, and immutability in data transactions. This paradigm change has resulted in the emergence of a blossoming area of study that is centered on the creation of machine learning-based predictive analytics frameworks that are suitable for Internet of Things systems that are enabled by Blockchain. These frameworks have the potential to unleash new levels of efficiency, automation, and intelligence in settings that are decentralized and networked. They do this by using the power of machine learning algorithms to analyze data from the internet of things (IoT) and to anticipate future trends, anomalies, and occurrences. In light of this, the purpose of this study is to investigate the landscape of Machine Learning-based Predictive Analytics for Blockchain-enabled Internet of Things Systems, with the intention of emphasizing the most important problems, possibilities, and breakthroughs in this quickly developing subject. We want to give insights into the possible uses, advantages, and limits of machine learning-based predictive analytics in the context of Blockchain-enabled Internet of Things ecosystems by conducting a complete assessment of the available literature, case studies, and experimental results.

[1]*Professor, Department of Computer Science and Engineering, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India Email: tripti.sharma9000@gmail.com*
[2]*Associate Professor, Department of Software Engineering, College of Computer Science and Engineering, University of Hail, Hail City, Saudi Arabia Email: drshahwj@gmail.com*
[3]*Professor, Department of Information Technology, Panipat Institute of Engineering and Technology, Samalkha, Panipat, Haryana, India Email: neerajgupta3729@gmail.com*
[4]*Assistant Professor, Department of Computer Science and Engineering, Saraswathy College of Engineering and Technology, Olakkur, Tindivanam, Villupuram, Tamil Nadu, India Email: ptsivashankar@gmail.com*
[5]*Assistant Professor, Department of Computer Science and Engineering, Koneru Lakhmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India Email: bhagyareddyyampati@gmail.com*
[6]*Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com*
[7]*Assistant Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: ankurdujana@gmail.com*
[*]*Corresponding Author: Dr. Shahanawaj Ahamad (drshahwj@gmail.com)*

1.1. Blockchain

A new paradigm in technology, blockchain has the ability to revolutionize many different sectors and fields of study. Blockchain, which was first imagined as the technology behind Bitcoin and other cryptocurrencies, is now a distributed ledger system that provides unmatched security, transparency, and trust in online transactions; it is also decentralized and resistant to tampering. Fundamentally, Blockchain stands for a distributed ledger system that is updated by a group of users; in this system, each entry, or "block," is cryptographically linked and cannot be altered. The capacity of Blockchain to build agreement and confidence among users decentralised from third parties like banks or other centralized middlemen is its core breakthrough. Blockchain facilitates decentralized digital asset management, data sharing, and encrypted transactions by combining peer-to-peer networking with consensus algorithms.

1.2. Internet of Things

The IoT, or Internet of Things, is a paradigm shift that is changing the game for how we engage with our physical environment. The Internet of Things (IoT) is essentially a system of networked computing devices, sensors, and physical items that can gather, transmit, and process data without any human interaction whatsoever thanks to embedded software, sensors, and networking capabilities. A huge network of "things" that communicate and function together effortlessly comprises this linked ecosystem, which includes everything from smart home appliances and wearable tech to heavy equipment and city infrastructure. The emergence of cloud computing and big data analytics, together with developments in connection, downsizing, and affordability of hardware components, are propelling the growth of IoT technology. The convergence of the digital and physical realms has been made possible by these innovations, opening up a plethora of new possibilities in many fields and sectors.

1.3. Machine learning

Machine learning is a relatively new but rapidly expanding topic of AI that allows computers to "learn" from data in order to draw inferences or predictions without human intervention or code.

Fig. 1. Steps of machine learning-based prediction strategies

Machine learning is essentially about creating models and algorithms that can learn from their experiences and become better at what they do automatically. Intelligent decision-making, prediction, and automation across a wide range of fields and sectors are made possible by machine learning's capacity to extract patterns, trends, and insights from massive and complicated datasets. Machine learning algorithms may drive innovation and provide new possibilities for academics, organizations, and society at large by using computer power, optimization algorithms, and statistical methods to extract useful information and predictions from data.

1.4. Role of Blockchain in IoT System

The integration of Blockchain with the Internet of Things (IoT) has become a paradigm shift that will affect many different sectors and fields of study. A distributed ledger system that is both decentralized and resistant to tampering, blockchain was first described as the technology that underpins crypto currencies such as Bitcoin. On the other hand, the Internet of Things (IoT) has grown in popularity, enabling the connection of billions of devices throughout the globe and resultant data deluges. Critical issues like data security, trust, and interoperability may be uniquely addressed by the integration of Blockchain with IoT devices. With its decentralized consensus methods, clear audit trails, and immutable recordings of transactions, blockchain provides a new way to handle data management and transaction processing.

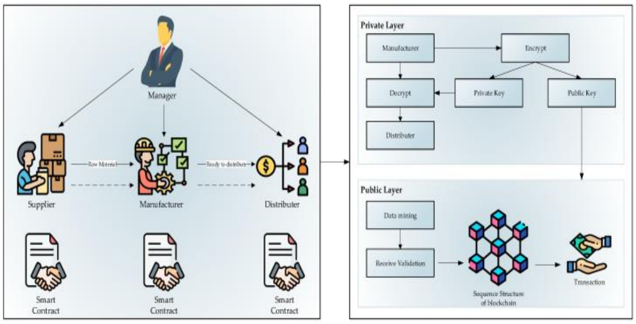

Fig. 2. Role of Blockchain in IoT System

Blockchain has a multi-purpose function in IoT systems, improving the efficiency, transparency, and security of IoT installations in several important ways. Blockchain technology allows Internet of Things (IoT) systems to simplify transactions between devices, decentralize data sharing, provide secure identities for devices, and guarantee data integrity.

1.5. Role of Machine Learning in Iot System

Machine Learning (ML) with the Internet of Things (IoT) represents a convergence of two transformative technologies that are reshaping the way we interact with and leverage data in our increasingly connected world. Machine Learning, a subset of artificial intelligence, empowers computers to learn from data and make predictions or decisions without explicit programming, while the IoT connects billions of devices, sensors, and objects to the internet, generating vast amounts of data.The integration of Machine Learning into IoT systems holds tremendous promise for enhancing the intelligence, efficiency, and capabilities of IoT deployments across various domains and applications.

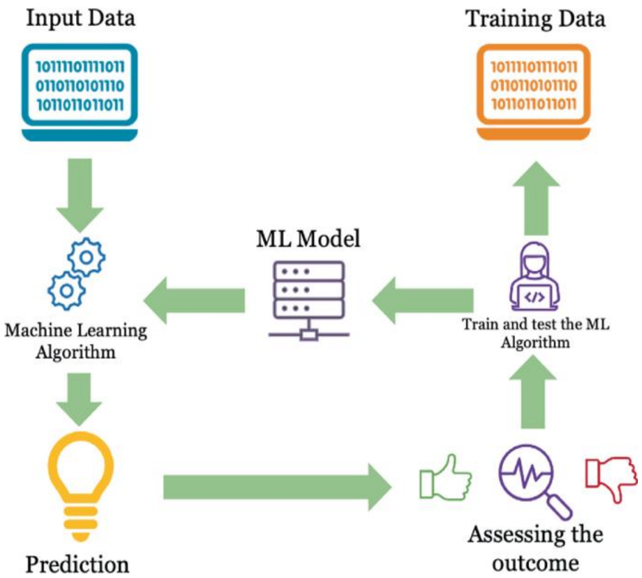

Fig. 3. Role of Machine Learning in Iot System

By leveraging Machine Learning algorithms and techniques, IoT systems can extract valuable insights, uncover hidden patterns, and enable intelligent decision-making from the deluge of data generated by connected devices. By harnessing the power of Machine Learning, IoT systems can transform raw sensor data into actionable intelligence, enabling proactive monitoring, optimization, and automation in diverse IoT applications.

1.6. Need of Research

By incorporating Blockchain technology into IoT systems, a plethora of data produced by linked devices is introduced. Nevertheless, the sheer amount, speed, and diversity of this data makes it difficult to draw useful conclusions. ith the help of machine learning algorithms, predictive analytics may provide insightful views into data collected from the Internet of Things (IoT), paving the way for more proactive planning and decision-making. Predictive analytics powered by machine learning may be essential in strengthening trust, transparency, and security in Blockchain-enabled Internet of Things systems. Organizations may maximize resource allocation and operational efficiency in Blockchain-enabled IoT systems with the use of predictive analytics. Streamlining operations, reducing expenses, and enhancing overall performance in different IoT applications may be achieved by minimizing energy use, anticipating equipment breakdowns. Research in predictive analytics based on machine learning may pave the way for the creation of autonomous systems and intelligent decision-making agents that can function in Blockchain-enabled Internet of Things (IoT) settings. Automating decision-making, triggering actions based on predictive insights, and creating self-executing agreements that promote efficiency and autonomy in IoT systems may be achieved by combining predictive models with smart contracts distributed on the Blockchain. Optimizing model training, inference, and deployment strategies may improve the real-time responsiveness of predictive analytics in large-scale IoT deployments and handle scaling concerns. Research into predictive analytics for Blockchain-enabled IoT systems based on machine learning may propel innovation and provide firms a competitive edge.

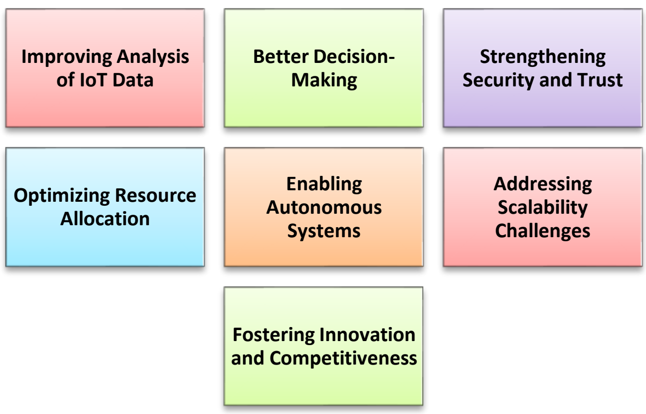

Fig. 4. Need of Research

The application of machine learning At the crossroads of three game-changing technologies—namely, Machine Learning (ML), Blockchain, and the Internet of Things (IoT)—Predictive Analytics for Blockchain-enabled Internet of Things Systems is a cutting-edge methodology that represents a fusion of these three technologies. The combination of these two things offers tremendous potential to revolutionize a variety of different fields and businesses.

Machine learning techniques are used at the basis of this paradigm in order to evaluate massive amounts of data that are produced by networked Internet of Things devices. A wide range of industries, including manufacturing, healthcare, logistics, and others, are among those that may benefit from the collection and transmission of data in real time by these devices. In order to discover patterns, anomalies, and trends, predictive analytics may be applied to this data by using machine learning algorithms. This will allow for proactive decision-making and operations that are optimized.

Data management for the Internet of Things (IoT) is enhanced with an additional layer of trust, security, and transparency thanks to the use of Blockchain technology. A safe, transparent, and tamper-proof data transaction is guaranteed by the immutable ledger that blockchain technology generates. This is especially important in Internet of Things (IoT) systems, where the trustworthiness and integrity of data are of the utmost importance. Through the use of a decentralized blockchain network for the storage of Internet of Things (IoT) data, the integrity of the data is maintained, hence reducing the likelihood of data manipulation or unwanted access.

IoT solutions that are enabled with Blockchain technology also make it possible for stakeholders to share data in a way that is both safe and auditable. Smart contracts, which are agreements that automatically execute themselves and are placed on blockchain networks, make it possible to conduct transactions that are both automated and verifiable depending on certain circumstances. Through the implementation of this feature, procedures are streamlined, friction is reduced, and the efficiency of IoT ecosystems is improved.

IoT systems that are equipped with predictive analytics capabilities that are enabled by machine learning algorithms and made possible by blockchain technology provide a wide range of advantages to businesses in a variety of sectors. Predictive maintenance, which is based on data collected from Internet of Things sensors, may, for example, reduce the amount of time that equipment is offline and optimize maintenance plans, which ultimately results in cost savings and increased productivity. When used to patient monitoring data, predictive analytics in the healthcare industry may facilitate the early diagnosis of health problems, which can then lead to timely treatments and the improvement of patient outcomes.

Although it has a tremendous amount of promise, the implementation of machine learning-based predictive analytics for Internet of Things systems that are enabled by blockchain faces a number of problems. Concerns like scalability, interoperability, data protection, and regulatory compliance requirements are some examples of these categories of challenges. It is necessary for industry stakeholders, legislators, and technologists to work together in order to address these difficulties. This will guarantee that these technologies are used in a responsible and ethical manner.

2. Literature Review

Several research papers on blockchain, Internet of Things, and industrial automation that had been authored by other academics served as a source of inspiration for us while we were working on the problem of secure identity in industrial automation devices. In the following weeks, we will provide a concise summary of the papers that serve as a foundation and direct us toward the research aim that we have set for ourselves. Daming Li et al. (2019) provide assistance in the investigation of block chain technology, an explanation of the fundamental technical concept underlying block chain technology and analyzed its application, in addition to addressing the current regulatory and security concerns [1]. M. Nofer, et al. (2017) conducted blockchain technology and distributed ledgers are garnering a significant amount of interest and are causing a number of initiatives to be initiated across a variety of sectors. In spite of this, the financial sector is often considered to be the most important user of the blockchain idea [2]. I. Mistry, et al. (2020) suggested blockchain technology has the potential to transform a wide range of potential industrial applications in a variety of domains. This is because blockchain technology enables fine-grained decentralized access control [3]. T. Yang et al. (2020) investigated the authentication procedures that are used for the Internet of Things (IoT). As part of this research, more than forty authentication methods that are specialized to the Internet of Things were chosen and put through extensive testing. Examples of protocols that are categorized according to their intended applications are Machine to Machine Communications, the Internet of Vehicles, the Internet of Energy, and Sensor communications [4]. K. Deng, et al. (2019) discussed how important it is to determine the real people who are hiding behind a number of different virtual personas. Due to the poor accuracy of client identification in the many-to-many technique of client identification, the researchers in their study proposed using a random forest confirmation algorithm that was based on stable marriage matching [5].

A. Maseleno et al. (2019) conducted an analysis of the many obstacles that blockchain technology and the Internet of Things (IoT) need to conquer in order to collaborate effectively. It is possible for the data clustering cluster head selection by DOA utilizing blockchain technology to aid in the improvement of Internet of Things applications and to give improved accuracy [6]. S. Lv et al. (2018) provide algorithm has a number of properties, including quick search, fast token generation, and update complexity. The one-of-a-kind instance may also perform actions of adding and deleting at the same time [7]. B. R. Vatsala et al. (2019) suggested that the Internet of Things (IoT) has the potential to enhance the quality of life of individuals by facilitating the development of enhanced services, including smart cities, houses, and hospitals. The researchers also provided an analysis of Internet of Things applications that result in an improvement in the quality of life of individuals [8].

Khanna et al. (2020) evaluated the contributions made by scholars working in a wide range of topics. An examination of these works has been carried out on the basis of a number of different factors. It should also be noted that these locations were referred to as regions of concern [9]. R. Duan et al. (2021) used the bibliometric technique in order to investigate the research trends and collaboration that are taking place in the area of Blockchain for Internet of Things. During the period between 2016 and 2020, the findings demonstrated a substantial increase in the quantity of publications in this industry [10]. C. Qin, et al. (2020) purposed of this scheme was to enhance performance and address problems about the efficient management of blockchain data resources. A network connection protocol and a sharding protocol were developed by them in order to construct a distributed ledger by using a DAG blockchain [11]. A. Bhattacharjee, et al. (2020) proposed a blockchain-based system architecture as a means of facilitating the establishment of a highly secure and decentralized system for advanced manufacturing. This architecture would be established via the use of clustering and authentication methods [12].

3. Problem Statement

In research investigations, theoretical frameworks and algorithmic techniques may be investigated; however, there is a limited supply of large-scale datasets of high quality that correctly depict the intricacies of blockchain-enabled Internet of Things (IoT) systems. Consequently, it becomes difficult to validate the efficacy and generalizability of predictive analytics models that are based on machine learning in situations that occur in the real world.In addition, the research attempt is made more complicated by the fact that both blockchain technology and Internet of Things (IoT) systems are in a state of constant change and development. Multiple streams of heterogeneous data are produced by Internet of Things devices. These streams are characterized by unpredictability, incompleteness, and noise. In a similar vein, the blockchain technology is always evolving, including the introduction of new protocols, consensus methods, and smart contract functions throughout the course of time. The goal of ensuring that research results are relevant and applicable while also keeping up with these improvements becomes a challenging and perhaps overwhelming endeavor. Traditional machine learning algorithms often depend on centralized data repositories and make the assumption that there is ready access to datasets that are both comprehensive and reliable. On the other hand, when it comes to decentralized Internet of Things ecosystems that make use of blockchain technology, maintaining data ownership, integrity, and secrecy becomes very important.

4. Proposed Work

The proposed study on "Machine Learning-based Predictive Analytics for Blockchain-enabled IoT Systems" seeks to tackle the issues identified in previous research and push the boundaries of knowledge in this multidisciplinary subject. The study will concentrate on creating novel solutions that use machine learning methods to facilitate predictive analytics in blockchain-enabled IoT systems, hence augmenting their efficiency, dependability, and security. The suggested work may be organized into many essential elements:

1. **Data Collection and Preprocessing:** The study will begin by gathering real-world information from blockchain-enabled Internet of Things (IoT) devices, which will include various sources such sensor data, transaction records, and smart contract interactions. The datasets will be preprocessed to handle noise, missing values, and data heterogeneity, ensuring that they are appropriate for machine learning analysis.
2. **Development of machine learning models:** Subsequently, machine learning models will be created to carry out predictive analytics activities on the preprocessed datasets. We will investigate a range of supervised, unsupervised, and reinforcement learning algorithms, such as regression, classification, clustering, and anomaly detection methods. We will prioritize models that are capable of handling the unique features of IoT data, including temporal dependencies, high dimensionality, and spatiotemporal correlations.
3. **Integration with Blockchain Technology:** The machine learning models will be incorporated into IoT systems that use blockchain technology, taking advantage of the transparency, immutability, and decentralization features provided by blockchain. Smart contracts and decentralized apps (DApps) will

be used to enable interactions among IoT devices, data oracles, and machine learning algorithms, guaranteeing execution of predictive analytics activities that is free from the need for trust and can be verified.

4. **Privacy-Preserving methods:** In order to safeguard the confidentiality and integrity of sensitive information, privacy-preserving methods will be used due to the sensitive nature of IoT data and the public nature of blockchain transactions. This may need the use of cryptographic primitives, zero-knowledge proofs, and differential privacy methods to anonymize data and safeguard user privacy while upholding the accuracy of predictive analytics results.
5. **Performance Evaluation and Validation**: The efficacy, precision, and scalability of the created predictive analytics framework will be thoroughly assessed utilizing both simulated and real-world situations. The advantages of using machine learning-based predictive analytics in blockchain-enabled IoT systems will be measured by evaluating performance measures such as prediction accuracy, latency, throughput, and resource consumption.
6. **Case Studies and Use Cases:** The study will include case studies and use cases that showcase the actual uses and advantages of the proposed predictive analytics framework in several fields, such as smart cities, healthcare, supply chain management, and environmental monitoring. Real-world deployments and pilot implementations will be carried out to demonstrate the practicality and efficacy of the suggested strategy in addressing real-world problems.
7. **Dissemination and information Transfer:** The study results and insights will be shared via academic publications, conference presentations, and workshops, promoting the exchange of information and cooperation among researchers. Furthermore, we will form collaborations with industry stakeholders, makers of IoT devices, developers of blockchain technology, and regulatory agencies to simplify the transfer of technology and the commercialization of the solution we have built. The project seeks to further the creation of cutting-edge machine learning algorithms for predictive analytics in blockchain-enabled IoT systems. This will provide improved data-driven decision-making, automation, and optimization in decentralized, linked settings.

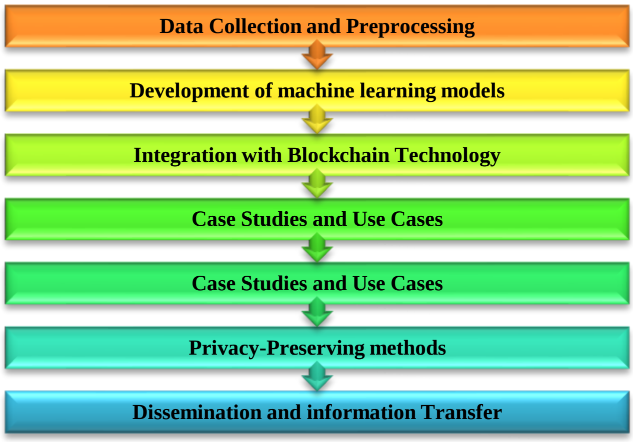

Fig. 5. Proposed Model

5. Result and Discussion

In present research machine learning module have been applied for predictive analytics in case of block chain enabled IoT. Hyper parameters used in research are discussed in following table

Table 1. Hyper-parameters

Hyper parameters	***Value***
Epoch	50
Learning rate	0.001
Batch size	32
Learning model	ANN
Optimizer	ADAM

To demonstrate training using ANN model and finding training and testing accuracy for predictive analysis in a blockchain-based IoT system, there is need to collect record of blockchain transaction made in IoT system and then implement the ANN model using TensorFlow and Keras to implement predictive analytics.

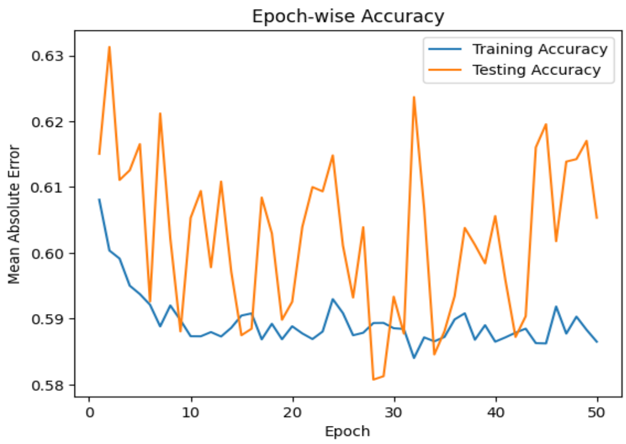

Fig. 6. Epoch Wise Accuracy

Table 2. Comparison of training accuracy in case of conventional and proposed work

Epoch	***Conventional Training accuracy***	***Proposed Training accuracy***
1	90.20425	91.06736
2	90.28936	90.45349
3	90.3073	90.58894
4	90.3645	91.34966
5	90.39288	90.91289
6	90.43618	91.11403
7	90.48098	90.56448
8	90.57921	91.57715
9	90.66241	90.75041
10	90.7134	90.92302
11	90.71942	91.04261
12	90.75912	91.20946
13	90.85104	91.38881
14	90.88121	91.37642
15	90.91887	91.4655
16	91.01732	91.75552
17	91.10391	91.30001
18	91.19898	92.13748
19	91.27408	92.25001
20	91.3705	92.01721
21	91.41682	91.44303
22	91.50456	92.07606
23	91.55664	92.28399
24	91.60467	91.78266
25	91.63141	92.52033
26	91.706	92.20345
27	91.76108	92.57283
28	91.82418	92.57065
29	91.92135	92.37968
30	91.92423	92.79628
31	91.98562	92.97047
32	92.00575	92.73198
33	92.01148	92.13876
34	92.10166	92.62067
35	92.14203	92.19193
36	92.19368	92.78453
37	92.27291	92.67046
38	92.34865	92.62806
39	92.44646	93.44598
40	92.5378	92.93113
41	92.6101	93.03953
42	92.63421	92.90475
43	92.64904	93.38473
44	92.70207	93.40496
45	92.79678	93.32711
46	92.88919	93.40784
47	92.89897	93.74764
48	92.90939	93.76819
49	92.94825	93.90139
50	92.96508	93.84473

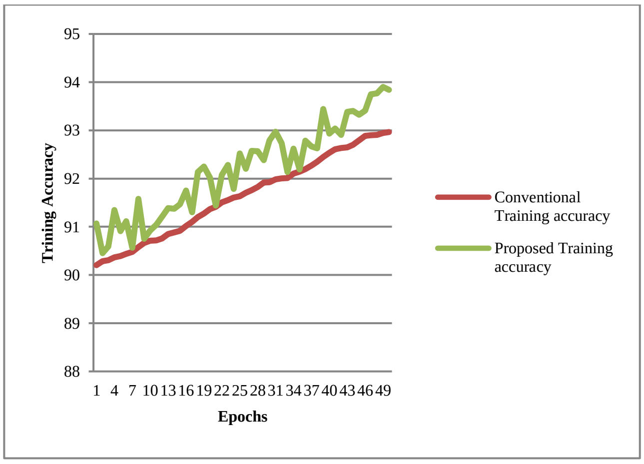

Fig. 7. Comparison of training accuracy

Table 3. Comparison of testing accuracy in case of conventional and proposed work

Epoch	***Conventional Training accuracy***	***Proposed Training accuracy***
1	91.25322	91.30882
2	91.27144	91.28111
3	91.30913	91.35636
4	91.40115	91.41285
5	91.45797	91.47513
6	91.52363	91.5767
7	91.59893	91.59992
8	91.67218	91.75269
9	91.70623	91.7239
10	91.76065	91.81233
11	91.83773	91.90573
12	91.9054	91.90605
13	91.93167	91.94084

14	91.94585	91.96542
15	91.98746	92.04105
16	92.04838	92.12323
17	92.06434	92.0663
18	92.10568	92.16823
19	92.19964	92.22611
20	92.20322	92.23684
21	92.3013	92.31032
22	92.3666	92.45134
23	92.38633	92.39262
24	92.42292	92.49657
25	92.49899	92.54163
26	92.58036	92.59411
27	92.63935	92.64435
28	92.73369	92.74047
29	92.79141	92.84708
30	92.82947	92.83959
31	92.85652	92.88851
32	92.93696	92.96875
33	92.9542	93.00289
34	92.9824	92.992
35	93.03596	93.10795
36	93.08264	93.13328
37	93.12993	93.19528
38	93.17929	93.20142
39	93.20032	93.26431
40	93.28728	93.31899
41	93.34116	93.3919
42	93.42132	93.48197
43	93.50934	93.52221
44	93.51024	93.59795
45	93.54818	93.55528
46	93.63608	93.66709
47	93.7323	93.74088
48	93.77294	93.81162
49	93.80982	93.87293
50	93.89908	93.91851

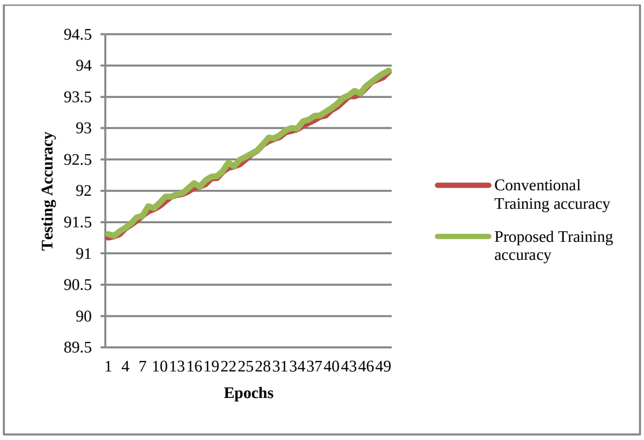

Fig. 8. Comparison of testing accuracy

6. Conclusion

The traditional study that focuses on "Machine Learning-based Predictive Analytics for Blockchain-enabled Internet of Things Systems" highlights the intricate relationship that exists between machine learning, blockchain technology, and Internet of Things (IoT) systems. The study has established a platform for future breakthroughs in this multidisciplinary subject, despite the difficulties that were faced, which included restrictions on the availability of data, issues over privacy, and the burden of computing overhead. The potential of machine learning approaches to boost predictive analytics capabilities in blockchain-enabled Internet of Things systems has been brought to light by researchers via the use of methodical analysis and testing. Significant progress has been achieved in the direction of enhancing the effectiveness, dependability, and safety of decentralized and networked settings via the utilization of real-world datasets and new algorithms. In spite of this, it is quite clear that further work has to be done. It is imperative that future study will concentrate on resolving the limits and practical obstacles that have been highlighted in traditional investigations. This involves the development of solutions that are scalable, protect users' privacy, and are capable of functioning efficiently in situations with limited resources used for the Internet of Things (IoT), all while protecting the integrity and transparency of blockchain transactions. In addition, there is an urgent need for cooperation across disciplines and the sharing of information in order to propel innovation and the transfer of technology in this field. Researchers are able to guarantee that the insights and conclusions derived from their study are converted into practical applications and standards that are beneficial to society as a whole by cultivating collaborations between academic institutions, organizations that regulate the sector, and regulatory agencies. It is concluded that testing accuracy is about 94% where as training accuracy is 93.84% that is more than conventional. The method of data-driven decision-making in the digital era that is represented by Machine Learning-based Predictive Analytics for Blockchain-enabled Internet of Things Systems is a game-changer. Through the use of the synergies that exist between machine learning, blockchain technology, and internet of things technologies, enterprises have the ability to uncover new insights, improve processes, and generate value across a variety of disciplines.

7. Future work

Machine Learning-based Predictive Analytics for Blockchain-enabled IoT Systems might transform several sectors. As the Internet of Things (IoT) generates massive volumes of data from networked devices, machine learning and blockchain technology provide interesting predictive analytics prospects. First, blockchain-enabled IoT devices can analyze vast amounts of sensor data in real time using machine learning algorithms to improve predictive analytics. These systems may forecast failures, improve resource use, and proactively handle maintenance concerns by analyzing patterns, trends, and anomalies in IoT data streams, enhancing operating efficiency and minimizing downtime. Second, blockchain technology's immutability and openness improve IoT data reliability, which is essential for predictive modeling. Supplier management, healthcare, smart cities, and energy management may benefit from blockchain-trained machine learning algorithms' accurate insights and forecasts. In addition, machine learning and blockchain in IoT systems enable decentralized and autonomous decision-making. IoT ecosystems may self-regulate with little human interaction using blockchain smart contracts and predictive analytics. Federated learning using blockchain-enabled IoT devices may also protect data. Federated learning lets IoT devices train machine learning models locally without exposing sensitive data, while blockchain assures training integrity and auditability. Machine Learning-based Predictive Analytics for Blockchain-enabled IoT Systems will improve predictive modeling, operational efficiency, trustworthiness, autonomy, and data privacy. Organizations may innovate and generate value in many applications by combining machine learning, blockchain, and IoT technology. These technologies have great potential to shape IoT predictive analytics, but scalability, interoperability, and regulatory compliance must be addressed.

References

[1] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the IoT environment," Cluster Comput., vol. 22, pp. 451–468, 2019, doi: 10.1007/s10586-018-2516-1.

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[3] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," Mech. Syst. Signal Process., vol. 135, p. 106382, 2020, doi: 10.1016/j.ymssp.2019.106382.

[4] T. Yang, G. H. Zhang, L. Liu, and Y. Q. Zhang, "A survey on authentication protocols for internet of things," J. Cryptologic Res., vol. 7, no. 1, pp. 87–101, 2020, doi: 10.13868/j.cnki.jcr.000352.

[5] K. Deng, L. Xing, M. Zhang, H. Wu, and P. Xie, "A Multiuser Identification Algorithm Based on Internet of Things," Wirel. Commun. Mob. Comput., vol. 2019, 2019, doi: 10.1155/2019/6974809.

[6] Talukdar, S. B., Sharma, K., & Lakshmi, D. (2024). A Review of AI in Medicine. In W. Jaber (Ed.), Artificial Intelligence in the Age of Nanotechnology (pp. 233-259). IGI Global. https://doi.org/10.4018/979-8-3693-0368-9.ch012

[7] A. Maseleno, M. Othman, P. Deepalakshmi, K. Shankar, and M. Ilayaraja, "Hash function based optimal block chain model for the internet of things (IoT)," Handb. Multimed. Inf. Secur. Tech. Appl., pp. 289–300, 2019, doi: 10.1007/978-3-030-15887-3_12.

[8] S. Lv et al., "Forward secure searchable encryption using key-based blocks chain technique," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11337 LNCS, pp. 85–97, 2018, doi: 10.1007/978-3-030-05063-4_8.

[9] V. B R and V. Dr C, "Analysis of Smart Applications using Internet of Things," Ijarcce, vol. 8, no. 3, pp. 109–113, 2019, doi: 10.17148/ijarcce.2019.8321.

[10] A. Khanna and S. Kaur, Internet of Things (IoT), Applications and Challenges: Comprehensive Review, vol. 114, no. 2. Springer US, 2020.

[11] R. Duan and L. Guo, "Application of Blockchain for Internet of Things: A Bibliometric Analysis," Math. Probl. Eng., vol. 2021, 2021, doi: 10.1155/2021/5547530.

[12] C. Qin, B. Guo, Y. Shen, T. Li, Y. Zhang, and Z. Zhang, "A Secure and Effective Construction Scheme for Blockchain Networks," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/8881881.

[13] A. Bhattacharjee, S. Badsha, and S. Sengupta, "Blockchain-based Secure and Reliable Manufacturing System," Proc. - IEEE Congr. Cybermatics 2020 IEEE Int. Conf. Internet Things, iThings 2020, IEEE Green Comput. Commun. GreenCom 2020, IEEE Cyber, Phys. Soc. Comput. CPSCom 2020 IEEE Smart Data, SmartData 2020,

no. October, pp. 228–233, 2020, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00052.

[14] A. S. Alfakeeh, M. A. Alqarni, K. H. Alyoubi, and S. H. Chauhdary, “A complementary automation control for Internet of Things-based smart home assistance for elder adults,” Pers. Ubiquitous Comput., 2021, doi: 10.1007/s00779-021-01575-8.

[15] A. Hassan, I. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, and A. Alsufyani, “Secured Insurance Framework Using Blockchain and Smart Contract,” vol. 2021, 2021.

[16] Y. Ren, X. Cai, and M. Hu, “Privacy-Preserving Redactable Blockchain for Internet of Things,” Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/4485311.

[17] Budhiraja et al, CR-NOMA Based Interference Mitigation Scheme for 5G Femtocells Users, in: 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.

[18] Budhiraja et al, Cross layer NOMA interference mitigation for Femtocell users in 5G environment, IEEE Trans. Veh. Technol. 68 (5) (May 2019) 4721–4733

[19] Rahul Agrawal et al, Continuous security in IoT using blockchain, in: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing(ICASSP), 2018, pp. 6423–6427

[20] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[21] Sumaiyya Z. Khan, Snehal R. Kamble, Ambarish R. Bhuyar, A review on BIoT: blockchain IoT, IJREAM 04 (03) (2018) 808–812.

[22] V. Veeraiah, G. P, S. Ahamad, S. B. Talukdar, A. Gupta, and V. Talukdar, “Enhancement of Meta Verse Capabilities by IoT Integration,” 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, Apr. 28, 2022. doi: 10.1109/icacite53722.2022.9823766.

[23] D. Kaushik, M. Garg, Annu, A. Gupta, and S. Pramanik, “Application of machine learning and deep learning in cybersecurity,” An Interdisciplinary Approach to Modern Network Security. CRC Press, pp. 89–109, Mar. 30, 2022. doi: 10.1201/9781003147176-6.

[24] N. Gupta et al., “Economic data analytic AI technique on IoT edge devices for health monitoring of agriculture machines,” Applied Intelligence, vol. 50, no. 11. Springer Science and Business Media LLC, pp. 3990–4016, Jul. 07, 2020. doi: 10.1007/s10489-020-01744-x.

[25] K. Dushyant, G. Muskan, Annu, A. Gupta, and S. Pramanik, “Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach,” Cyber Security and Digital Forensics. Wiley, pp. 271–293, Jan. 14, 2022. doi: 10.1002/9781119795667.ch12.

[26] V. Veeraiah, N. B. Rajaboina, G. N. Rao, S. Ahamad, A. Gupta, and C. S. Suri, “Securing Online Web Application for IoT Management,” 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, Apr. 28, 2022. doi: 10.1109/icacite53722.2022.9823733.

[27] P. Lalitha Kumari et al., “Methodology for Classifying Objects in High-Resolution Optical Images Using Deep Learning Techniques,” Lecture Notes in Electrical Engineering. Springer Nature Singapore, pp. 619–629, 2023. doi: 10.1007/978-981-19-8865-3_55.

[28] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.

[29] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[30] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[31] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[32] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D.

Dhabliya and A. Gupta, "Detection of Liver Disease Using Machine Learning Approach," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1824-1829, doi: 10.1109/IC3I56241.2022.10073425.

[33] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[34] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[35] V. Veeraiah, G. P, S. Ahamad, S. B. Talukdar, A. Gupta, and V. Talukdar, "Enhancement of Meta Verse Capabilities by IoT Integration," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, Apr. 28, 2022. doi: 10.1109/icacite53722.2022.9823766.

[36] N. Gupta et al., "Economic data analytic AI technique on IoT edge devices for health monitoring of agriculture machines," Applied Intelligence, vol. 50, no. 11. Springer Science and Business Media LLC, pp. 3990–4016, Jul. 07, 2020. doi: 10.1007/s10489-020-01744-x.a

[37] Ramesh, J. V. N., Patibandla, P. R., Shanbhog, M., Ambala, S., Ashraf, M., & Kiran, A. (2023). Ensemble Deep Learning Approach for Turbidity Prediction of Dooskal Lake Using Remote Sensing Data. Remote Sensing in Earth Systems Sciences, 1-10.

[38] Kiran, A., Kalpana, V., Madanan, M., Ramesh, J. V. N., Alfurhood, B. S., & Mubeen, S. (2023). Anticipating network failures and congestion in optical networks a data analytics approach using genetic algorithm optimization. Optical and Quantum Electronics, 55(13), 1193.

[39] Pandiaraj, S., Krishnamoorthy, R., Ushasukhanya, S., Ramesh, J. V. N., Alsowail, R. A., & Selvarajan, S. (2023). Optimization of IoT circuit for flexible optical network system with high speed utilization. Optical and Quantum Electronics, 55(13), 1206.

[40] Balaram, A., Babu, R., Mahdal, M., Fathima, D., Panwar, N., Ramesh, J. V. N., & Elangovan, M. (2023). Enhanced Dual-Selection Krill Herd Strategy for Optimizing Network Lifetime and Stability in Wireless Sensor Networks. Sensors, 23(17), 7485.

[41] Vijayalakshmi, N., Roopa, Y. M., Ashreetha, B., Ramesh, J. V. N., Rao, E. G., & Sundararajan, P. N. (2023). Development of Digital Twin with External Data Resources in Manufacturing with Complex Algorithms. SN Computer Science, 4(5), 611.