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

Securing Digital Records: A Synergistic Approach with IoT and Blockchain for Enhanced Trust and Transparency

Sinjan Kumar[1], Md. Ehtashamoul Haque[2], Raj Kumar[3], Neeraj Gupta[4,*], Vuyyuru Lakshma Reddy[5], Dr. Thalakola Syamsundararao[6], Dharmesh Dhabliya[7]

Submitted: 22/11/2023 **Revised**: 28/12/2023 **Accepted**: 07/01/2024

Abstract: In the age of accelerating digitalization, digital record security and integrity are crucial across businesses. This article proposes using IoT and Blockchain technologies to improve digital record security, authenticity, and transparency. This technique combines IoT devices for data collection with blockchain for secure, decentralized, and tamper-proof record-keeping to build trust and transparency in the digital ecosystem. With its network of linked devices, the Internet of Things generates real-time data. When combined with digital documents, this data provides a complete and verifiable history. Blockchain's decentralized and immutable ledger secures digital record recording and validation. IoT and Blockchain work together to solve data integrity, security, and transparency issues. This study examines how IoT and Blockchain might safeguard digital records in healthcare, supply chain, banking, and other areas. Case studies and use-cases show how this synergistic approach improves traceability, lowers fraud, and assures digital record dependability in trust-critical situations. The paper also examines scalability, interoperability, and regulatory compliance issues related to this strategy. Adopting a complete IoT and Blockchain framework for digital record security requires understanding and solving these concerns. As digital transformation changes businesses, digital documents must be secured. This article discusses a collaborative method that uses IoT and Blockchain to establish a safe, transparent, and trustworthy digital record-keeping infrastructure. By adopting this synergistic paradigm, companies can confidently traverse the digital terrain and protect their digital records.

Keywords: *Security, IoT, Blockchain, Trust and Transparency, Digital Records, Synergistic Approach*

1. Introduction

At a time when digitization has grown pervasive, the integrity and security of digital records are essential components in order to fulfill the requirements of trust and transparency that are needed across a variety of industries. This study investigates a cutting-edge method for bolstering digital records by integrating two revolutionary technologies, namely the Internet of Things (IoT) and Blockchain, in a way that creates a synergistic effect. This approach seeks to establish a robust framework that not only improves the safety of digital records but also guarantees an unprecedented level of trust and transparency in the digital realm. This is accomplished by combining the capabilities of the Internet of Things (IoT) to generate data in a continuous manner with the secure and decentralized characteristics of Blockchain.

The Internet of Things has brought about a revolution in the process of data collection by delivering a constant stream of information available in real time from devices that are linked to one another. In light of the fact that this data is becoming more and more important, it is very necessary to guarantee its safety and validity inside digital records. Blockchain, which is well-known for its immutable and decentralized ledger, emerges as a logical partner to the Internet of Things (IoT) in order to solve problems linked to the integrity of data and the recording of safe transactions. The complementary nature of these technologies offers the possibility of developing an all-

[1]*Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, Vaishali, Bihar, India Email: sinjan.dtu@gmail.com*
[2]*Assistant Professor, Department of Computer Science and Engineering, B.P.Mandal College of Engineering, Madhepura, Bihar, India Email: ehtasham47@gmail.com*
[3]*Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, Vaishali, Bihar, India Email: nit.er.raj@gmail.com*
[4]*Professor, Department of Information Technology, Panipat Institute of Engineering and Technology, Samalkha, Panipat, Haryana, India Email: neerajgupta3729@gmail.com*
[5]*Assistant Professor, Department of Computer Science and Engineering, Koneru Lakhmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India Email: lakshmareddy@kluniversity.in*
[6]*Associate Professor, Department of CSE- Data Science, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India Email: syamsundar.jes@gmail.com*
[7]*Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India Email: dharmesh.dhabliya@viit.ac.in*
[*]*Corresponding Author: Neeraj Gupta (neerajgupta3729@gmail.com)*

encompassing solution that can satisfactorily solve the ever-evolving issues posed by the environment of digital technology.

Within the context of protecting digital records across a variety of sectors, this study investigates the practical uses of the collaborative potential of the Internet of Things (IoT) and Blockchain. By means of case studies and use cases, we investigate several situations in which this synergistic approach improves traceability, decreases the likelihood of fraud, and creates a new benchmark for the trustworthiness of digital record-keeping.

1.1. Role of IoT in Digital Record Security

Digital record security has been greatly strengthened as a result of the integration of the Internet of Things (IoT), which has also introduced a paradigm change in the way that companies approach the integrity and confidentiality of their data. Internet of Things (IoT) devices, which may range from sensors to smart gadgets that are linked to one another, are an essential component in the generation of a continuous stream of real-time data. This amount of information not only improves the granularity of digital records, but it also offers an excellent source for monitoring and identifying irregularities in the data. For instance, Internet of Things (IoT)-enabled medical equipment contribute to the safe monitoring of patient data in a healthcare context. This helps to ensure that vital health information is kept correct and unmodified. On the other hand, this proliferation of data also presents issues, which calls for the implementation of stringent cybersecurity measures to protect against the possibility of vulnerabilities and unwanted access points. However, despite these challenges, the incorporation of the Internet of Things (IoT) into digital record security presents opportunities that have never been seen before to strengthen data protection. These opportunities enable organizations to respond proactively to emerging threats and to maintain the trust and confidentiality of digital records in a landscape that is becoming increasingly interconnected.

1.2. Blockchain as a Foundation for Secure Record-Keeping

Blockchain technology is a fundamental pillar in the field of safe record-keeping. It offers a decentralized and immutable ledger that dramatically improves the security and integrity of digital information. Blockchain technology acts as a basic pillar. When records, also known as blocks, are cryptographically linked and stored across a network of nodes, a blockchain is created. This ensures that once a block is added, it becomes almost impossible to alter the existing information. The distributed structure of the blockchain minimizes the vulnerability that is associated with centralized databases, hence lowering the chance of hostile attacks or unauthorized changes being made to the data. Each member in the blockchain network has a copy of the whole ledger, which contributes to the system's transparency and creates a system in which consensus is necessary for any modifications to be made. When it comes to businesses like banking, where the integrity of transactions is of the utmost importance, the secure and transparent nature of blockchain technology guarantees an indelible record of financial transactions can be maintained. In addition, the decentralized design reduces the likelihood of a single point of failure, which in turn strengthens the resistance of record-keeping systems to the effects of cyberattacks. It is becoming more apparent that the use of blockchain technology as a secure basis for record-keeping is a solution that is both transformational and resilient. This is because companies are working to protect their data from the rapidly growing security concerns.

1.3. Synergistic Integration of IoT and Blockchain

A strong alliance in the field of digital record security is formed by the synergistic integration of the Internet of Things (IoT) and Blockchain. This alliance offers a complete solution that meets the difficulties of data integrity, transparency, and trust resulting from the integration of these two technologies. The potential of the Internet of Things (IoT) to create real-time data via the use of networked devices is in perfect harmony with the fundamental concepts of Blockchain. Organizations are able to establish a comprehensive framework for the safekeeping of records by merging the constant data streams that are generated by Internet of Things devices into a decentralized and immutable ledger. By ensuring that the information that is gathered by Internet of Things devices is not only saved safely but also verifiable and tamper-proof, this integration contributes to an increase in the dependability of digital records. In the context of a supply chain, for instance, Internet of Things sensors have the capability to send real-time information on the movement of items, while blockchain technology guarantees that every transaction is legally recorded and can be traced. A trustworthy and auditable trail of events is established as a result of the transparent and decentralized nature of the integrated Internet of Things and Blockchain system. This not only protects digital information from being accessed or altered by unauthorized parties, but it also reinforces the integrity of the systems. This collaborative approach reshapes the way in which industries maintain and safeguard their digital records. It provides a foundation that is both durable and transparent, which instills trust in the authenticity and dependability of digital data.

1.4. Applications Across Industries

1. **Healthcare: Ensuring Data Integrity in Patient Records**

Within the realm of healthcare, the combination of Internet of Things (IoT) and Blockchain technology plays a crucial

part in assuring the authenticity and safety of patient information. Wearable health monitors and other technologically advanced medical gadgets are examples of Internet of Things devices that continually produce real-time health data. When this information is combined with a blockchain-based system, it generates a record of a patient's medical history, treatments, and results that is both secure and unchangeable. It is possible for healthcare professionals to make use of this technology in order to improve the accuracy of data, speed medical processes, and guarantee that patient records are not vulnerable to illegal adjustments. Not only does this result in an improvement in the quality of treatment provided to patients, but it also brings about a foundation of trust within the healthcare ecosystem.

2. Supply Chain: Digitally Traceability and Transparency

When used to the management of supply chains, the Internet of Things (IoT) and Blockchain technology bring about new levels of traceability and transparency with their combined strength. The Internet of Things (IoT) sensors that are implanted in goods and shipments offer real-time data on the location, condition, and other environmental conditions of the individual items. The blockchain, which functions as an immutable ledger, records every transaction and movement that takes place in the supply chain in a safe manner. Through the use of this synergy, stakeholders are able to track the route of goods from the point of manufacture to the point of distribution, hence assuring authenticity and compliance at each milestone. In the end, the players in the digital supply chain will have more faith in one another as a result of the increased responsibility, decreased likelihood of fraudulent activity, and more transparency that this integration provides.

3. Finance: Fraud Reduction and Secure Transactions

Within the realm of finance, the joint integration of Internet of Things (IoT) and Blockchain technology makes a contribution to the reduction of fraudulent activity and the formulation of safe transaction ecosystems. Internet of Things (IoT) technologies, such as biometric sensors and smart cards, improve systems for verifying identities, hence lowering the likelihood that unauthorized individuals would get access to financial documents. The creation of an immutable record of each and every transaction is one of the ways that Blockchain technology simultaneously protects the safety and transparency of financial transactions. Not only does this reduce the likelihood of fraudulent operations, but it also makes international transactions easier to complete in a more expedient and secure manner. The use of Internet of Things (IoT) and Blockchain technology in the financial sector not only protects sensitive financial information but also revolutionizes the efficiency and dependability of national and international financial institutions.

In addition, the research takes into account the difficulties and important factors that are linked with the execution of this collaborative method. When it comes to the smooth implementation of a comprehensive Internet of Things and Blockchain architecture, scalability, interoperability, and regulatory compliance are essential issues that need consideration.

The protection of digital records and the verification of their validity are becoming non-negotiable aspects of business operations as we move into an age in which companies are becoming more and more dependent on digital records. In order to give insights into a forward-looking strategy that harnesses the capabilities of the Internet of Things (IoT) and Blockchain, the purpose of this paper is to establish an infrastructure that not only protects digital records but also promotes trust and transparency. By adopting this synergistic paradigm, businesses are able to boldly begin on their paths toward digital transformation, secure in the knowledge that their digital records will be reliable and accurate.

2. Literature Review

There are several research projects now being conducted in the field of big data and blockchain technology, all of which are mentioned in this section. It was highlighted by Naveen Rishishwar et al. (2017) that in this day and age, data is of the biggest significance for each and every firm, organization, and industry, including those that are just beginning their operations. Everyone may benefit from having access to data when it comes to making important decisions that are pertinent to their growth. In the event that there is an increase in the amount of the data that is greater than the constraint.When the size of the database increases to the point that it becomes extremely difficult to administer using the traditional database software, this is the ideal situation. In the following step, we referred to it as "Big Data." In terms of computing, scalability, storage, and processing, large volumes of data provide a variety of diverse challenges that must be addressed. Big Data allows for the efficient management, storage, and processing of large volumes of data in a manner that is very efficient. Additionally, Big Data is responsible for managing the massive number of data. This is done in order to have the capability of extracting relevant information from such a large quantity of data in order to help with decision-making. It is a well-known truth that a significant amount of businesses are not utilizing Big Data. This is mostly owing to the fact that there are a variety of issues and challenges that need to be tackled. Within the scope of this study, the key challenges and obstacles that are now being encountered with Big Data were specifically emphasized. Not only that, but we also discussed a variety of various strategies for coping with them [1]. In order to enhance the process of selecting the initial center points and the method

for calculating the distance from other locations to the center point, you should propose a privacy and availability data clustering (PADC) scheme that is founded on the k-means algorithm and differential privacy. This is the recommendation that was made by J. Xiong et al. (2019). In addition, PADC makes an effort to reduce the influence of the outlier effect by recognizing outliers during the clustering process. This serves to reduce the impact of the outlier effect. Based on the findings of the security study, it has been determined that our approach is effective in accomplishing the goal of differentiated privacy and in preventing the disclosure of personal information. The performance evaluation, on the other hand, reveals that our approach, while preserving the same level of privacy, does a better job of increasing the availability of clustering results in contrast to the differential privacy k-means algorithms that are currently being utilized. This demonstrates that the PADC scheme that we have developed is better to other systems that are used to provide intelligent electricity service by utilizing the Internet of Things [2]. In the year 2020, V. R. Niveditha and colleagues offered a framework of big data as a means by which methodologies of static and dynamic malware detection may be successfully coupled in order to reliably classify and identify zero-day malware. This framework is provided as a means by which this combination can be effective. This framework has been evaluated and evaluated on a sample file set of 0.1 million, which includes clean files of 0.03 million and contains a wide variety of malware families that total 0.13 million dangerous binaries. The framework has been tested and estimated on this sample file set. The findings suggest that supporting vector machines (SVM) attained the maximum degree of accuracy, which was 93.03%, when it came to recognizing malware and benign sorts [3]. This was accomplished through the utilization of 10-fold cross validation. According to Abdulbaset Salem et al. (2021), the term "big data" refers to a new paradigm in the field of technology that comprises data that is generated at a quick speed, in vast numbers, and with a wide variety of features. It is being touted as a revolution that has the potential to totally revolutionize the way businesses operate across a wide range of industries, and massive volumes of data are being praised as contributing to this revolution. This article offers a brief introduction to big data as well as a discussion of the various aspects that comprise data quality. The challenges that are linked with the quality components of big data are also discussed, as is the longevity of big data analytics [4]. In addition, it examines the lifetime of big data analytics. A methodology for the analysis of massive amounts of data pertaining to Internet of Things (IoT) household devices was presented by J. Jung et al. (2019). These gadgets are provided to customers through a number of distribution methods, are employed by house users in smart houses, and are maintained at A/S centers, which are frequently considered to be repair shops. The distribution stage, the customer-usage stage, and the A/S stage are the three key phases during which we collect a substantial quantity of data and do an analysis of that data. The framework that has been presented for the purpose of providing support to small and medium-sized firms in the process of building an elastic strategy for the new product is the ultimate aim of the framework. Because of this, they are able to arrive at a conclusion that is more successful at three crucial stages of the process. As an illustration, they are able to reduce the amount of duplication that is present in relation to a distribution route, in addition to modifying the quantity of storage, release, and stock [5]. NFT culture is the name given to the way of life that was provided by 9NFTMANIA, according to the research that was carried out by Gupta, M. et al (2023). Within this society, non-fungible tokens (NFT) would be used for a variety of purposes, including but not limited to greetings, invitations, certificates, and membership cards. By doing things in this way, it would be feasible to perform a secure transfer of digital assets, and this non-fungible token would have a certain value. The sending of non-fungible tokens (NFT) to the wallet of another individual is something that should be done regardless of whether the individual desires to convey thanks to another individual or simply wish them a good morning. Furthermore, there would be a restriction placed on the supply of such greeting NFT, which would mean that there is still the chance of an increase in the price of the purchase. On the other side, when web 3.0 methods are used to validate NFT holders in Metaverse, people who have NFT would be able to gain access to premium online services [6]. This would be possible as NFT holders would be verified. M. Gupta et al. (2023) presented blockchain technology, and since then, NFTs (Non-Fungible Tokens) have attracted a significant degree of interest, particularly in the field of digital assets and decentralized technology. The popularity of these two concepts has increased in tandem with their strong relationship to one another. Blockchain technology serves as the foundational technology that enables non-fungible tokens (NFTs) to function as one-of-a-kind digital assets. This link between blockchain and NFTs (Non-Fungible Tokens) is mutually beneficial. On the other hand, non-fungible tokens, also known as NFTs, are a form of digital currency that use blockchain technology to solve the age-old challenge of proving ownership and validity in the digital realm. Non-fungible tokens, also known as NFTs, are a solution to the problem of digital scarcity. They have the ability to overcome this problem by representing unique assets on the blockchain. This enables creators, such as musicians, game developers, and artists, to tokenize their digital creations and sell them as limited-edition, one-of-a-kind items [7]. Tokenization is a form of digital asset management. The setting of decentralized finance

ecosystems was examined by R. Gupta et al. (2023), and they mentioned that liquidity pools are a key component in the process of preserving the value of tokens. The use of arbitrage is one of the most important ways in which liquidity pools assist to the maintenance of stability. One of the most important contributing processes that liquidity pools are involved in is this one. In situations where the value of a token is low, purchasers will make purchases. When, on the other hand, the item is priced at a higher than normal level, sales are made accessible. Arbitrage is made possible by the presence of liquidity pools, which enable traders to carry out these transactions directly on decentralized exchanges. This makes arbitrage a very viable activity. This makes arbitrage a company that can be successful. The continual pressure imposed by arbitrageurs adds to the token's value reverting to its target peg, which in turn serves to cultivate additional stability [8]. In their discussion of the findings of the research that was conducted, D. Gupta and colleagues (2023) came to the conclusion that the most important aspect that impacts the value that is given to greetings is the degree of popularity that they enjoy. In addition to this, it has been found out that the Love Emogie is only accessible in a restricted quantity. The growing demand for non-fungible tokens (NFTs) has been a contributing element from the limited availability of just 43 Love Emojie. This is because of the inherent scarcity of non-fungible tokens (NFTs). On the other hand, it is important to point out that the concerns of cost and use case have a considerable influence [9]. Pi Network is a cryptocurrency project that was proposed by R. Issalh and colleagues in 2023. Pi Network is notable for the innovative approach it takes to mining and accessibility. Users of the site, which was launched in 2019, are provided with the opportunity to mine the network's native digital money, which is known as Pi, straight from their mobile devices. By democratizing the mining process and making participation in cryptocurrency more accessible to a larger variety of individuals, the platform aims to accomplish its goals. Especially interesting is the fact that the block chain that Pi Network uses is constructed on the Stellar Consensus Protocol. This protocol places equal priority on the concepts of security, decentralization, and transaction speed. Participation from the community is given a substantial amount of importance by Pi Network, which is still in the beginning stages of its growth. [10] It encourages people to actively join in the project and contribute to it by providing them resources. An investigation of the importance of non-fungible token avatars in the metaverse was carried out by A. Duggal and colleagues (2023). The researchers focused specifically on the role that these avatars play in redefining digital ownership, self-expression, and user engagement. In addition to this, the research investigates the challenges and obstacles that are associated with the marketing of NFT avatars. It takes into account a wide range of factors, such as the dynamics of the market, the challenges posed by technology, and the adoption of the product by users. The research that is being conducted takes into account a wide range of non-fungible tokens (NFTs) that have been developed by a variety of various NFT Brands. It is possible that this NFT will be utilized in the Meta verse at some point in the future. An NFT referred to as the "Sizzling monster" has been the subject of a case study that has been developed at the end of the research paper. A number of non-fungible token (NFT) firms have previously acquired it from Young Parrot Platform at the beginning of its existence [11]. The availability of this NFT is extremely limited. The recommendation made by M. Gupta et al. (2023) to desist from engaging in speculation in the cryptocurrency market during NFT transactions is a call to exercise prudence, conduct study, and commit to responsible investment. The acceptance of these principles will contribute to the formation of an ecosystem that is more trustworthy and sustainable, which will eventually make it possible for the block chain technology that supports it to achieve its promise beyond the narrow scope of short-term market fluctuations. It is necessary to have a strategy that is both cautious and well-informed while engaging in speculation in the cryptocurrency market, particularly when dealing with transactions that use non-fungible tokens (NFT). There is a significant amount of intrinsic volatility in the cryptocurrency market, which is exacerbated by the non-fiat currency region. This is one of the most noticeable aspects of the cryptocurrency market. It is vital for investors to exercise prudence and resist from giving in to the temptation of speculating since prices are prone to unexpected and unpredictable shifts. This is because of the fact that prices are prone to movements that are not predictable. The value of non-fungible tokens (NFTs) is not decided by conventional fundamentals; rather, it is controlled by factors like as the perceived scarcity of the tokens, the demand for them, and the cultural importance of the tokens [12].

3. Problem Statement

Securing digital records through the synergistic approach of integrating IoT and Blockchain, while promising enhanced trust and transparency, encounters a set of formidable challenges. One central issue revolves around the scalability of both technologies. As the volume of data generated by IoT devices continues to escalate, ensuring that the blockchain network can accommodate and process this influx of information poses a significant scalability challenge. Scaling blockchain to handle the growing demands of a comprehensive IoT ecosystem requires innovative solutions to maintain efficiency and effectiveness. Interoperability concerns constitute another critical challenge. Integrating various IoT devices and blockchain platforms within an interconnected framework

demands a standardized approach. Ensuring seamless communication and data exchange among diverse devices and blockchain systems is essential for the success of this synergistic model. Developing standardized protocols and fostering collaboration among different stakeholders become imperative to overcome interoperability hurdles. Moreover, the security of IoT devices represents a significant concern in this context. As endpoints of data collection, IoT devices are vulnerable to cyber threats. Ensuring the robustness of the entire system requires implementing stringent security measures for both IoT devices and the blockchain infrastructure. Any compromise in the security of IoT endpoints could potentially undermine the integrity and trustworthiness of the entire digital record-keeping system. Ethical considerations surrounding data privacy and ownership are crucial aspects that demand careful navigation. Balancing the benefits of enhanced transparency with the need to protect sensitive information and uphold individual privacy rights is a complex challenge. Striking the right balance between transparency and privacy within the context of a synergistic IoT and Blockchain framework is crucial for building and maintaining trust among users. Addressing these challenges in securing digital records through a synergistic IoT and Blockchain approach requires a comprehensive strategy that encompasses technological innovation, regulatory frameworks, and industry collaboration. As organizations strive to fortify the trust and transparency of digital records, they must navigate these challenges to unlock the full potential of the combined power of IoT and Blockchain technologies.

4. Proposed work

Through the use of deep learning, there are many phases involved in the classification of digital documents for security purposes. According to this process flow, the following are the primary steps of this task:

1. Obtaining a big dataset of digital assets, including their metadata, transaction history, ownership details, and any other pertinent information, is the first step in the data collection process. It is important to make sure that the dataset is both varied and representative, including a wide range of digital different assets.

2. Data Preprocessing: Clean and preprocess the data that your organization has collected. In order to do this, it may be necessary to deal with missing values, normalize numerical features, encode categorical variables, and solve any other data quality problems that may arise. Get the data ready for additional examination if you will.

3. Feature Extraction: Take the digital dataset and extract the characteristics that are important to the problem. Metadata features, transaction patterns, ownership changes, and other factors that are essential for clustering might be included in this category. The extraction of features is an essential step in the process of providing the deep learning model with relevant input.

4. Selecting an Appropriate Deep Learning Model: When clustering, it is important to select an appropriate deep learning model. Autoencoders and variations of autoencoders, such as Variational Autoencoders (VAEs), are frequently utilized for problems involving unsupervised feature learning and clustering. When it comes to collecting intricate patterns in high-dimensional data, these models are just what the doctor ordered.

5. Model Training: Train the previously chosen deep learning model by making use of the digital data that has been preprocessed. The model should be given the opportunity to discover patterns and representations in the data without being given explicit labels, and unsupervised learning approaches should be utilized. Training the model to encode the input data in a space with fewer dimensions is something that has to be done.

6. Dimensionality Reduction: In order to lessen the complexity of the learnt features, it is necessary to use certain approaches for dimensionality reduction. It is imperative that this phase be completed in order to adequately see and analyze the clusters. It is possible that methods such as t-Distributed Stochastic Neighbor Embedding (t-SNE) might be helpful in accomplishing this objective.

7. Implement a clustering technique on the lower-dimensional representations that were acquired from the deep learning model. This is the seventh step in the process. K-means, hierarchical clustering, and DBSCAN (Density-Based Spatial Clustering of Applications with Noise) are examples of methods that are often utilized for clustering.

8. Analysis of the Security Situation: An examination of the clusters' security should be carried out. Conduct a thorough analysis of the features of each cluster in order to recognize any trends, irregularities, or potential security risks. In order to do this, it may be necessary to search for odd transaction patterns, changes in ownership, or other behaviors that may suggest potential security problems.

Remember that the success of this process relies on the quality of the data, the choice of deep learning model, and the effectiveness of the clustering algorithm. Additionally, staying informed about the latest developments in the Digital record space and adapting the clustering model

accordingly is crucial for maintaining security in dynamic environments.

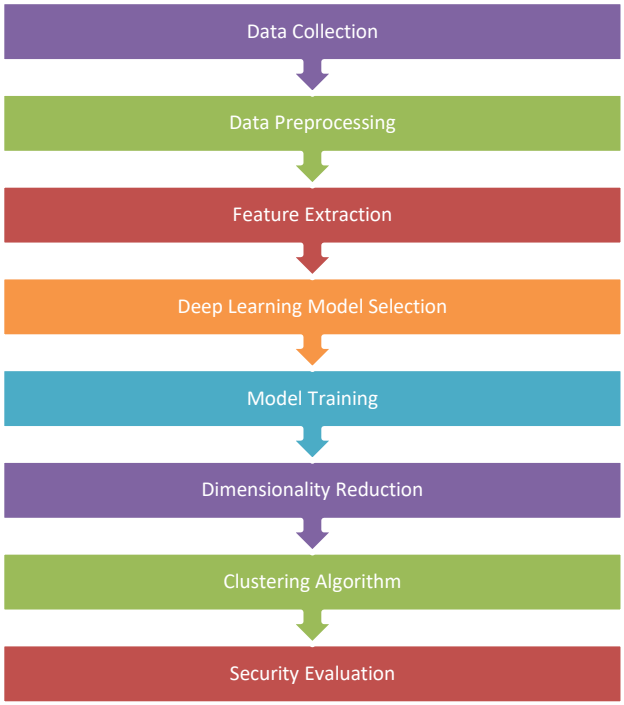

Fig 1 Process flow of classification of digital record for security using deep learning

5. Result and Discussion

Different aspects of digital data, such as the total supply, the creator, the name, the rate, the description, the contract address, and the transaction information, are taken into consideration during the simulation phase. Using deep learning, clustering has been created for four different groups in order to ensure the safety of digital information.

5.1 Simulation of Proposed Deep Learning

For the simulation of the suggested deep learning model, there are two categories to choose from. A complete evaluation procedure is required in order to generate a confusion matrix following the training of digital data connected with digital records in the context of security. To begin, the clustering model is trained with large-scale datasets that include information connected to digital records. These datasets include transaction records, ownership details, and other qualities that are pertinent to the problem at hand. The purpose of this endeavor is to discover any inherent patterns, relationships, or abnormalities that may be present within the digital data and that may be indicative of possible dangers or problems connected to security. Following the completion of the model training, the subsequent stage consisted of constructing a ground truth for the purposes of assessment. This ground truth might be produced from recognized clusters or classifications that are present in the dataset, or it could be found using domain expertise and external evaluation procedures. Both of these ways are possible. It is possible that the review process will incorporate qualitative assessments carried out by subject matter specialists in the event that obvious ground truth labels are not available. Following the establishment of the ground truth, the trained clustering model is applied to the 9nftmania (9NM) dataset, and each data point is assigned to a cluster that has been predicted during the process. After that, the confusion matrix is created, which offers a tabular representation of the performance of the model by comparing the predicted clusters with the actual cluster assignments. This matrix makes it possible to evaluate the model's capacity to reliably detect patterns or groups that may suggest aberrant activity, potential fraud, or security threats. This evaluation may be carried out in the context of security. Several different assessment measures, each of which provides a different perspective on the performance of the clustering model, are derived from the confusion matrix, which acts as the foundation for these metrics. In the course of calculations, metrics including as precision, recall, F1 score, and accuracy are frequently utilized. The F1 score is a metric that combines precision and recall into a single metric. Precision is a measurement of the accuracy of positive predictions, recall is a measurement of the capacity to catch all positive occurrences, and the F1 score combine the two. Refinement and enhancement of the model are both possible because to the iterative nature of the clustering assessment process. It is possible to make modifications to hyperparameters, algorithms, or the entire architecture of the model based on the insights that are obtained from the confusion matrix and the metrics that are linked with it. When it comes to ensuring that the model is successful in recognizing security-related trends within the ever-changing ecosystem of 9nftmania token, continuous monitoring and frequent review are both essential components. In general, this methodology makes it easier to conduct a methodical and data-driven evaluation of the effectiveness of the clustering model in terms of improving the level of security achieved inside the domain of digital records.

Table 1 Confusion matrix of Conventional Deep learning model

	Success	**Failure**
Success	976	15
Failure	24	985

Results

TP: 1961

Overall Accuracy: 98.05%

Table 2 Accuracy parameters for Conventional deep learning model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1000	991	98.05	0.98	0.98	0.98
2	1000	1009	98.05	0.98	0.98	0.98

After simulating conventional deep learning model

proposed hybrid simulation has been made to find the confusion matrix.

Table 3 Confusion matrix of Proposed Deep learning model

	Success	Failure
Success	983	6
Failure	17	994

Results

TP: 1977

Overall Accuracy: 98.85%

Table 4 Accuracy parameters for proposed deep learning model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1000	989	98.85%	0.99	0.98	0.99
2	1000	1011	98.85%	0.98	0.99	0.99

5.2 Comparative analysis of accuracy parameters

Considering table 1 and table 2 comparative analysis of accuracy parameters such as recall, precision, F1-score has been made in this section.

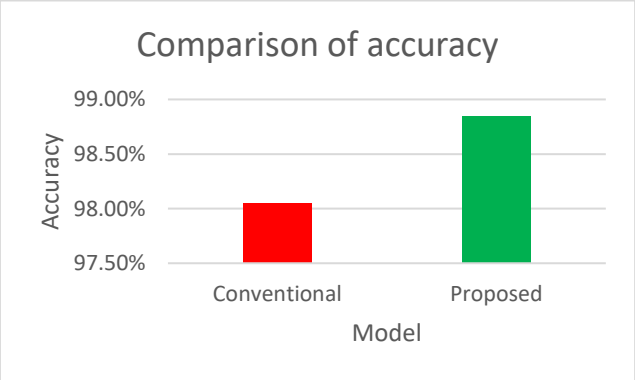

Fig 2 Comparison of Accuracy

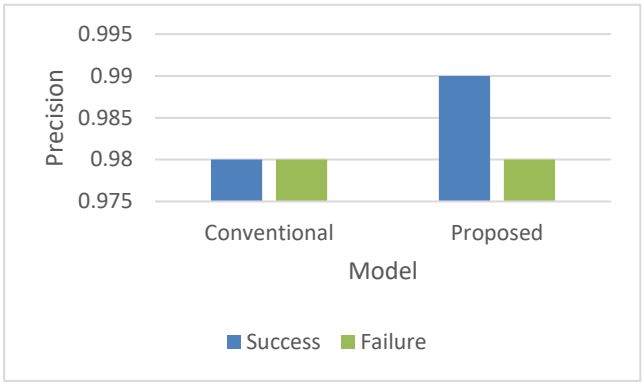

Fig 3 Comparison of precision

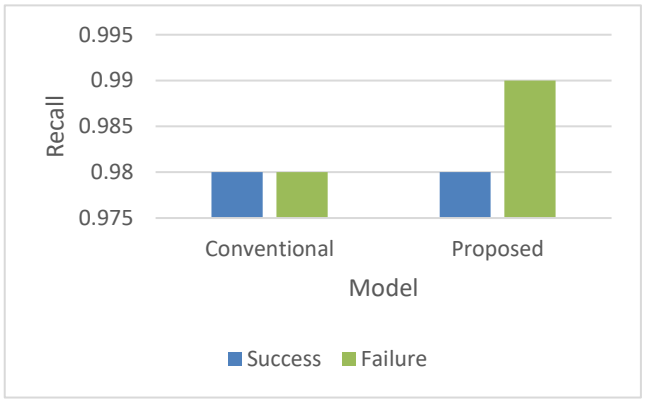

Fig 4 Comparison of Recall

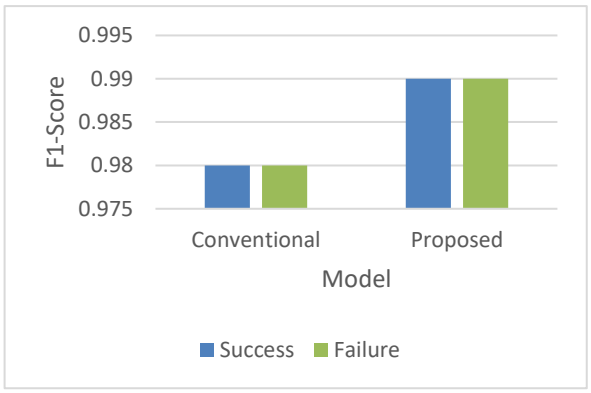

Fig 5 Comparison of F1-Score

6. Conclusion

Simulation results conclude that the script considered in present paper is 9NFTMANIA has been classified with better accuracy in case of proposed work as compared to conventional approach. Error rate in case of proposed work is less whereas accuracy in case of present research is more than that of conventional approach.

7. Future scope

The future scope of securing digital records through a synergistic approach with IoT and Blockchain holds immense promise, presenting a trajectory towards unprecedented trust and transparency in digital ecosystems. As both IoT and Blockchain

technologies continue to advance, their integration is poised to become more seamless, robust, and adaptable to a myriad of industries beyond their current applications. One aspect of the future scope lies in addressing the scalability challenge. Innovations and optimizations in blockchain protocols and consensus mechanisms, coupled with advancements in IoT data processing, will likely pave the way for the efficient handling of exponentially increasing data volumes. Interoperability will be a focal point for development, as the integration of diverse IoT devices and blockchain platforms becomes more prevalent. Standardized protocols and collaborative efforts within the industry will be essential to ensure that different systems can seamlessly communicate and share data, fostering a cohesive and interconnected digital ecosystem. The future will also witness heightened emphasis on security measures, particularly focusing on enhancing the resilience of IoT devices against evolving cyber threats. Innovations in cryptographic techniques and decentralized identity management within the blockchain framework will contribute to creating a more robust defense against potential vulnerabilities, reinforcing the trustworthiness of the entire system. Ethical considerations and regulatory frameworks will likely evolve to address the complex landscape of data privacy and ownership. Striking a balance between transparency and individual privacy rights will be crucial, and the development of clear guidelines and regulations will play a pivotal role in shaping the ethical dimensions of this synergistic approach. In essence, the future scope of securing digital records through IoT and Blockchain integration envisions a landscape where data is not only secure and transparent but also seamlessly interconnected across various applications and industries. As these technologies mature, their collaborative potential is poised to redefine the standards of trust and transparency, creating a digital infrastructure that is not only resilient to emerging challenges but also aligned with evolving ethical considerations in the digital age.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Naveen Rishishwar, Vartika, Mr. Kapil Tomar (2017, march). Big Data: Security Issues and Challenges. International Journal of Technical Research and Applications, e-ISSN: 2320-8163, Special Issue 42 (AMBALIKA), PP. 21-25.

[2] J. Xiong et al. (2019, april). Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1530-1540.

[3] V. R. Niveditha, T. V. Ananthan , S.Amudha Dahlia Sam and S.Srinidhi(2020), Detect and Classify Zero Day Malware Efficiently In Big Data Platform.

[4] Abdulbaset Salem Albaour, Yousof Abdulrahman Aburawe (2021). Big Data: Review Paper.

[5] J. Jung, K. Kim and J. Park(2019), Framework of Big data Analysis about IoTHome-device for supporting a decision making an effective strategy about new product design, International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 2019, pp. 582-58

[6] Gupta, M., Gupta, D., & Duggal, A. (2023). NFT Culture: A New Era. Scientific Journal of Metaverse and Blockchain Technologies, 1(1), 57–62. https://doi.org/10.36676/sjmbt.v1i1.08

[7] M. Gupta, “Reviewing the Relationship Between Blockchain and NFT With World Famous NFT Market Places”, SJMBT, vol. 1, no. 1, pp. 1–8, Dec. 2023.

[8] R. Gupta, M. Gupta, and D. Gupta, “Role of Liquidity Pool in Stabilizing Value of Token”, SJMBT, vol. 1, no. 1, pp. 9–17, Dec. 2023.

[9] M. GUPTA and D. Gupta, “Investigating Role of Blockchain in Making your Greetings Valuable”, URR, vol. 10, no. 4, pp. 69–74, Dec. 2023.

[10] R. Issalh, A. Gupta, and M. Gupta, “PI NETWORK : A REVOLUTION”, SJMBT, vol. 1, no. 1, pp. 18–27, Dec. 2023.

[11] A. Duggal, M. Gupta, and D. Gupta, “SIGNIFICANCE OF NFT AVTAARS IN METAVERSE AND THEIR PROMOTION: CASE STUDY”, SJMBT, vol. 1, no. 1, pp. 28–36, Dec. 2023.

[12] M. Gupta, “Say No to Speculation in Crypto market during NFT trades: Technical and Financial Guidelines”, SJMBT, vol. 1, no. 1, pp. 37–42, Dec. 2023.

[13] A. Singla, M. Singla, and M. Gupta, “Unpacking the Impact of Bitcoin Halving on the Crypto Market: Benefits and Limitations”, SJMBT, vol. 1, no. 1, pp. 43–50, Dec. 2023.

[14] Gupta and P. Jain, “EXPECTED IMPACT OF DECENTRALIZATION USING BLOCKCHAIN BASED TECHNOLOGIES”, SJMBT, vol. 1, no. 1, pp. 51–56, Dec. 2023.

[15] D. Gupta and S. Gupta, “Exploring world famous NFT Scripts: A Global Discovery”, SJMBT, vol. 1, no. 1, pp. 63–71, Dec. 2023.

[16] V. Veeraiah, H. Khan, A. Kumar, S. Ahamad, A. Mahajan and A. Gupta, "Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 713-718, doi: 10.1109/ICACITE53722.2022.9823883.

[17] M. Gupta, “Integration of IoT and Blockchain for user Authentication”, SJMBT, vol. 1, no. 1, pp. 72–84, Dec. 2023.

[18] A. Singla and M. Gupta, “Investigating Deep learning models for NFT classification : A Review”, SJMBT, vol. 1, no. 1, pp. 91–98, Dec. 2023.

[19] A. Gupta, R. Singh, V. K. Nassa, R. Bansal, P. Sharma and K. Koti, "Investigating Application and Challenges of Big Data Analytics with Clustering," 2021 International Conference on Advancements in

Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675483.

[20] Mamta, V. Veeraiah, D. N. Gupta, B. S. Kumar, A. Gupta and R. Anand, "Prediction of Health Risk Based on Multi-Level IOT Data Using Decision Trees," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 652-656, doi: 10.1109/ICSEIET58677.2023.10303560.

[21] 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), Greater Noida, India, 2022, pp. 1499-1504, doi: 10.1109/ICACITE53722.2022.9823733.

[22] K. A. Shukla, S. Ahamad, G. N. Rao, A. J. Al-Asadi, A. Gupta and M. Kumbhkar, "Artificial Intelligence Assisted IoT Data Intrusion Detection," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[23] 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.

[24] 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), Greater Noida, India, 2022, pp. 1493-1498, doi: 10.1109/ICACITE53722.2022.9823766.

[25] 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.

[26] D. Mandal, K. A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161

[27] K. A. Shukla, V. Juneja, S. Singh, U. Prajapati, A. Gupta and D. Dhabliya, "Role of Hybrid Optimization in Improving Performance of Sentiment Classification System," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 541-546, doi: 10.1109/PDGC56933.2022.10053333.

[28] 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.

[29] 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.

[30] V. Veeraiah, V. Talukdar, S. B. Talukdar, J. Kotti, M. K. Dharani and A. Gupta, "IoT Framework in a Blockchain dependent Cloud Environment," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308158.

[31] Pandey, J.K., Ahamad, S., Veeraiah, V., Adil, N., Dhabliya, D., Koujalagi, A., Gupta, A. Impact of call drop ratio over 5G network (2023) Innovative Smart Materials Used in Wireless Communication Technology, pp. 201-224.