FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

Simulating Hybrid Deep learning mechanism for security enhancement during Blockchain based WSN authentication

Tejbir Singh[1], Rohit Vaid[2]

[1,2]*Department of Computer Science & Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to Be University), Mullana, Ambala, Haryana, India;* tejbirrana662@gmail.com[1] , rohit.vaid1@gmail.com[2]

*Correspondence: *tejbirrana662@gmail.com*

ABSTRACT- In wireless sensor networks, sensor nodes have constrained resources including processing speed, memory, and battery life. WSNs are susceptible to a broad range of vulnerabilities since they are often used in untrusted environments. Given the difficulties of securing a WSN, the reliability of the information it collects is also put into question. WSNs' authentication procedure permits checks on the legitimacy of both resources and data. Data in WSNs is protected against tampering thanks to authentication, which checks the data's provenance and allows only authorized changes. However, current authentication methods have certain security holes, such as those that may be exploited by ID spoofing attacks. When it comes to cyber security, blockchain is another example of a promising new technology. All transactions on the blockchain are cryptographically protected and cannot be altered once they have been made. The goal of this study is to one day use blockchain technology in wireless sensor networks (WSNs). In this research, we created a novel authentication procedure for WSNs that relies on blockchain technology. Users and a private blockchain were important in integrating sensor nodes and the blockchain into the study's system architecture. The study's data was subjected to a thorough examination for security. Deep learning model has been used to classify secure and unsecure record over blockchain based WSN. Classification of data stored on blockchain is made after performing filtering using optimizer.

Keywords: Blockchain, WSN, Security, WiSeN sensor node, Deep learning, Performance, Authentication Method, Optimization.

ARTICLE INFORMATION

Author(s): Tejbir Singh, Rohit Vaid;

Received: 16/02/2023; **Accepted**: 21/03/2023; **Published**: 30/09/2023;
e-ISSN: XXXX-XXXX;
Paper Id: IJCSR-030104;
Citation: 10.37391/IJCSR.030104

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

To monitor Earth's condition, scientists have developed WSN, or wireless networks made up of numerous sensor nodes. WSN are used in several fields, from the domestic to the industrial to the transportation sectors, and more. There might be hundreds of applications in each class. Example applications in environmental science include measuring water quality, keeping an eye on forest fires, and maintaining tabs on farmland. Gardens and stadiums are ideal environments for wireless sensor networks due to their limited size. However, they also have a variety of uses in the wild, such as border patrol and fire control.

2. BLOCKCHAIN

To put it simply, a "blockchain" is a cryptographically linked, immutable record of past transactions. In distributed ledgers, a network of nodes or processes connects these keys or signatures. The network guarantees that all nodes are constantly using the most up-to-date copy of the whole chain. There are several advantages to using blockchain technology, as stated by NIST. These include the impossibility of backdating transactions and the decentralized nature of blockchain digital ledgers. The technological advancement has been given the name "DLT" due to its useful properties. Medical records and other sensitive information should not be kept on a public blockchain where anybody may see the information. In light of increased transparency, providers must pay careful thought to user privacy to safeguard sensitive data. To start, it's important to remember that blockchain technology already has safeguards to completely do away with hacking. Due to the fact that blockchain is open source, it might be vulnerable to attacks by hackers and social engineers. Thus, information security is crucial in any industry, but especially in healthcare.

Figure 1: Blockchain

3. WSN

To gather and communicate data from sensors monitoring environmental or physical elements like noise or vibration, a WSN is employed. Multiple wireless sensors may form a WSN, or wireless sensor network, to monitor a system's or an area's status remotely. Environmental monitoring is a key function of WSNs, which are networks of sensors spread out across a wide

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

area. Temperature and wind speed are two examples of environmental elements that WSNs could monitor. Like wireless ad hoc networks, they depend on wireless connectivity and the spontaneous extension of networks to enable wireless transfer of sensor data. WSNs are able to pick up on environmental or physical variables such as temperature, sound, and pressure. These days, networks do more than just transport data; they also provide control over sensor behaviour. The military's primary motivation for establishing these networks is the need to monitor military fields. These networks have numerous useful and consumer-facing uses, from monitoring the condition of equipment to controlling operations in factories.

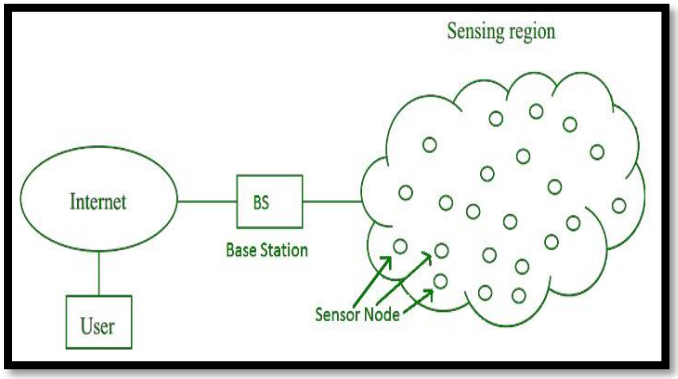

Figure 2. Wireless Sensor network

2. RELATED WORK

Ant Colony optimization was capable to solving the job scheduling problems. Were the job scheduling is related to the scheduling performance, response time and the completion time. Several Multi-Objective optimization scheduling also contains the completion time, commercial cost and energy consumption. Ant Colony Optimization permits fast near optimal results to be found. It is useful in industrialized surroundings where computational resources and time are limited. Scheduling method used Ant colony optimization method to solve this problem.

2.1 Scheduling Performance

The best essential features for schedulers is the entire processing time of cloud job. The main target of scheduling performance is scheduling time. Some researcher uses intelligent optimization algorithms to optimize job scheduling. The focus in on decreasing time, response time, completion time related with scheduling performance. The scheduling problems divided into two portions: the variety discovery and advance discovery. To explain addiction of cloud jobs, the scheduling problems can be interpreted into the directed acyclic graph (DAG).

2.2 The Multi-Objective Optimization Scheduling

Multi-objective optimization comprises the completion time, Quality of service (QoS), energy consumption and economic cost. In cloud computing there are many elements to be used for job scheduling. Multi-Objective optimization way has been projected difference metrics like cost, resource utilization. Energy consumption also the major problem for maintenance of cloud datacenters. The main target of multi-objective optimization algorithms are execution time, economic cost, and system performance. The use of a multi objective optimization in job scheduling is minimizing make span and cost in a multi cloud environment. It proposed a multi-objective optimization method to exploit the income of cloud providers.

2.3 Scheduling Method Based On ACO Algorithm

Italian scholar M.Dorigo proposed the Ant Colony Optimization algorithm to resolve the ideal result of combinatorial optimization problem. The optimization scheduling problems comprises several targets of performance and cost. Firstly, this scheduling method focused on scheduling productivity, such as accomplishment time. It is generally emphases on optimizing the total implementation time by ant colony optimization algorithm using guesstimate method. The scheduling method grounded on ant colony optimization method. By using pre-execution time that works set of pheromone threshold to avoid the local optimum solution. Secondly the system performance works not only reduces make span but also achieve the load balancing by decreasing the time. The ant colony optimization algorithm schedules the jobs of cloud customers to virtual machines in cloud computing environment in an effective way. The ACO algorithm solve the over-all optimization problem with ant by evading the extended paths whose pheromones are incorrectly collected by leading ants.

Thirdly the scheduling method consider the cost. For example an ant colony optimization algorithm solves the tricky by using big workflow arrangement and various quality of service factors. Mainly the scheduling methods estimate the quality of the result and the performance and cost.

3. SYSTEM MODEL

A wireless sensor network (WSN) is a network in which each "node" is a sensor node and the number of nodes may vary from few to several thousand. Each node has an electrical circuit for linking the sensors, a CPU, a power source (often a battery or an incorporated form of energy harvesting), and a radio transceiver with an antenna. It's conceivable that one day sensor nodes the size of a dust particle will be feasible, but we're not there yet. A sensor node might cost anything from a few dollars to several hundred, depending on its sophistication. Size and cost constraints place constraints on available resources such power, storage, processing speed, and data transfer rates. There are several possible topologies for WSNs, from the simplest "star" networks to the most complex "multi-hop" wireless mesh networks. Both routing and flooding are practical means of establishing contact.

4. SECURITY

Encryption is the practice of encoding information with the use of secret techniques. With this strategy, we may transform data from its unencrypted form into a secure one. Only approved

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

parties should be able to decipher cypher messages to ensure the security of confidential information. Encryption may prevent data from being understood by an unauthorized user, but it cannot prevent it from being intercepted. This method generates a pseudo-random encryption key that may be used in practice. It takes a lot of time, effort, and knowledge to crack a well-designed encryption method without the key. Using the key provided by the sender, the message can be deciphered only by the receiver. A third party could never use it to access the encoded information. The practice of using encryption to safeguard private data has grown widespread. It is possible to use cryptography to deliver a message that can only be decoded by the intended receiver and sender. Intercepted communications may be read and decoded by anybody from the outside who has the required information. Polynomial encryption will be used in the proposed research, and it will be compared to standard techniques of data encryption like RSA and AES.

4.1 RSA

One of the most common ways to safeguard data transmission is with the help of the Rivest-Shamir-Adleman (RSA) public-key cryptosystem. It's also one of the oldest languages in the world. The RSA algorithm was initially described in public by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. The initials "RSA" were derived from their surnames. British mathematician Clifford Cocks was responsible for the 1973 clandestine creation of a similar system at the British signals intelligence agency, Government Communications Headquarters (GCHQ). This technology was first introduced to the general public in 1997. While the public may get their hands on the encryption key, the decryption key is kept hidden under a public-key cryptosystem.

4.2AES

The U.S. National Institute of Standards and Technology (NIST) produced the Advanced Encryption Standard (AES), formerly known as Rijndael, in 2001 as a standard for the encryption of digital data. During the AES selection process, two Belgian cryptographers, Joan Daemen and Vincent Rijmen, proposed a variation of the Rijndael block cypher to NIST. Various key and block sizes are available for the Rijndael family of cyphers. NIST settled on Rijndael, a family of algorithms having a block size of 128 bits and key lengths of 128, 192, and 256 bits for AES. U.S. federal agencies now use AES. The Data Encryption Standard (DES), first released in 1977, has been replaced by this newer standard. Since the same key is used for both encryption and decryption, AES is considered a symmetric-key method. On November 26, 2001, the National Institute of Standards and Technology (NIST) officially adopted AES as U.S. FIPS PUB 197. The Rijndael cypher was chosen after a five-year standardisation process in which fifteen other designs were submitted and evaluated. ISO/IEC 18033-3 includes support for AES. After being approved by the U.S. Secretary of Commerce on May 26, 2002, AES officially became a federal government standard in the United States. When used with an NSA-approved cryptographic module, AES is the first and only publicly available cypher certified for use with classified material by the United States National Security Agency (NSA).[note 4]

4.3 Role of Blockchain in WSN

The security and reliability of conventional WSNs are enhanced by a BWSN system because it does away with the necessity for a TTP. When it comes to storing sensory data, you can rely on BWSN's distributed system. Thus, there is no need to worry about the SPF problem. The widespread use of blockchain technology in crypto currencies has sparked investigations into its potential applications in wireless networks, where it may facilitate honest transactions between parties that were previously unknown to one other. One of the many possible uses for blockchain technology is ensuring the integrity of data sent across a wireless body area network. Each wireless node in a WSN is also a sensor, so the network may collect information about its immediate surroundings. A gateway server PC facilitates communication between the WSN and the rest of the Internet. The gateway server has the potential to exert influence over any individual node.Blockchain, one of the newest technologies, has shown to be a trustworthy network. When used in trustworthy WSN apps, blockchain technology has the potential to foil the efforts of cybercriminals who send phishing or other spoofed communications to consumers. Smart contract and blockchain-based authentication and access control solutions for networks are conceivable. In addition, malicious actors are naturally attracted to targets with a centralized security strategy. Therefore, many strategies might be used to get the vital center. The distributed nature of blockchain applications, however, may make this threat less severe.

4.4 Role of Security in WSN

Participants in a blockchain transaction may claim ownership of their data by using private and public keys. No one is authorized to have access to this information. If private data is stored on a blockchain, its owners may set permissions to control who can access it and under what conditions. One of the biggest challenges of WSNs is meeting strict security criteria while making do with minimal resources. WSN security requires node authentication, data confidentiality, compromise resistance, and analysis of traffic resistance. Many security and privacy issues are brought up by multi-hop routing. Spying, sinkholes, modified Sybils, clones, wormholes, spoofing, etc. are just a few examples of issues that might undermine the security and privacy of WSNs. WSNs monitor things like temperature, noise, and pressure in the surrounding environment. In addition to data collecting, modern networks also facilitate the administration of sensor output. The military's need for applications like battlefield surveillance led to the development of such systems.

4.5 Authentication of BWSN

Using authentication may help prevent these security flaws [2]. Data authentication in sensor networks checks that information has originated from reliable sources and prevents data from being altered once it has been collected. Secure communication between nodes in WSNs is impossible without authentication. Authentication is used to verify that the two sensor nodes communicating to each other are indeed genuine.

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

Authentication guarantees that only authorized sensor nodes will be able to join the network. With this strategy, only authorized users may connect to the system. Authenticating users in WSNs may be done in many different methods. Authentication may be accomplished in a number of methods, including using user IDs, CP, MAC addresses, and passwords. Unfortunately, the presently used techniques have their drawbacks. ID spoofing attacks might compromise authentication techniques that rely on a user's unique identifier. Certificate-based authentication solutions have a significant memory and processing cost on sensor nodes. The reliability of an authentication technique that uses a certain encryption protocol is proportional to the robustness of that protocol. Incontestable techniques of proving identification include MAC address authentication and password-based authentication. The rigorous authentication technique will ensure that only authorized sensor nodes are added to the network. Data manipulation, non-repudiation, message replay, man-in-the-middle attacks, and denial of service must be resisted by strong defenses.

4.6 Motivation for research

The shortcomings of the existing authentication methods, as well as the advantages of the proposed technology, have led to a focus on the need of incorporating it into the WSN. Blockchain has the potential to revolutionize WSN, but there are a number of challenges that must be addressed before it can be used. However, blockchain demands a lot of processing power and energy, and the WSN has limited capacity nodes. The blocks on the blockchain will need more and more room as the number of executed transactions increases. While this is a step in the right direction, more has to be done before WSN applications can take use of the extremely secure properties of blockchain technology. For this reason, a new blockchain-based authentication mechanism tailored to secure WSN applications has been developed. Analyses of the proposed protocol's security and efficiency were positive. This study indicates not only a high degree of security but also efficiency in terms of latency, energy, and memory use.

4.7 Paper organization

Section 1 has introduced WSN security in term of blockchain and elaborated motivation for research
Section 2 is presenting the conventional research that are under taken in area of WSN and Blockchain
Section 3 is problem statement part where issues of conventional research are elaborated.
Section 4 has discussed proposed work
Section 5 is focused on result and discussion
Section 6 is presenting conclusion of simulation
Section 7 focused on future scope of research

4.8 Literature Review

There have been several research in area of blockchain and WSN. Research methodology used in conventional approach has been discussed here.

Gautam, A.K. et al. (2021) reviewed in-depth analysis of wireless sensor network key management, authentication, and trust management practices. In this article, they conducted a comprehensive literature review on the use of trust management, authentication, and key management scheme features. They discussed the techniques, benefits, and drawbacks of the existing key management, authentication, and trust management scheme in WSN based on their evaluation. The purpose of this in-depth research was to analyze available security options and settle on the one that best serves the needs of the application. Additionally, the frontiers that could be pushed to achieve the finest security solutions in the future were included, along with their strengths, shortcomings, and open challenged [1].

Nguyen, C.V et al. (2021) looked the Pros and Cons of Using Blockchain Technology in WSNs. Blockchain (BC) was one of the newest distributed technologies now in use. Blockchain, as a distributed ledger technology, may improve the efficiency and safety of computation and administration of WSNs. In this post, they take a looked at how Blockchain technology might be used to WSN and the advantages and disadvantages of do so. They draw the conclusion that Blockchain technology may provide a viable solution to the issues of security and distributed storage for WSN. This might lead to excited new avenues of study and decentralized uses[2].

Arivarasi, A et al. (2021) reviewed the honey encryption method based on adaptive trust sectors for better source location privacy protection in WSN.An environment and its matched item may be identified with the use of a wireless sensor network, which was a collection of sensor nodes. It takes in every detail of the scenario and sends them on to the main node through wireless connection. However, there were obstacles to overcome in wireless sensor networks, such as the effective placement of sensor nodes. Energy scarcity, transmission capacity, range, data dispersion, data permanence, malfunctioned nodes, and data security redundancy were just a few of the problems that need to be solved. The apps have been monitored using a signed version of the Discovery Configuration Protocol (DCP). It's vital for secondary uses, which need recreating the original data source [3].

Sureshkumar, C et al. (2021) did research on energy-efficient fuzzy-based authentication and clustering algorithm for wireless sensor networks.In order to prevent assaults, the Fuzzy-based Secured Authentication and Clustering (FSAC) Algorithm was proposed here. This algorithm takes into account the variety of sensor data packets. The FSAC was used to reduce power consumption by selecting the most efficient routed route. Using fuzzy logic, this technique locates the neighbor transmitter to optimize data packet routing route configuration. According to the simulation find, the suggested strategy may boost energy production by as much as 12% compared to similar approaches [4].

Yavari, M et al. (2020) enhanced IoT network administration with a blockchain-based authentication protocol. An enhanced blockchain-based authentication protocol (IBCbAP) was also presented by their team, complete with security feature included secure access management and anonymity. They used the JavaScript programming language and Ethereum for the local blockchain to create IBCbAP. We have provided

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

formal and informal security proof for IBCbAP using the Scyther tool. They found that IBCbAP could provide enough protection at a cost that was manageable [5].
Uddin, M.A et al. (2019) considered the minimalist blockchain-based infrastructure for the oceanic internet of things.Their proposed solution employs a Fog and Cloud architecture with many layers to safely process and store data from IoUT devices using adapted Blockchain technology. IoUT data is safely sent across the network's hierarchical structure, guaranted the reliability of all collected information. The design was put through a series of tests to ensure its safety and performance, and the results showed that it was able to safely and effectively gather data from IoUT devices in the monitoring area[6].

Dong, S et al. (2020) introduced secure mobile device authentication in the IoT using blockchain technology.Inthis work, they present a blockchain-based authentication method that might be used in many domains. Using the cosmic network model, this approach ensures that portable devices may always connect to networks outside of their current domain. Their experiment validate the viability of this approach and show that it outperforms competing cross-domain authentication methods [7].

Goyat, R et al. (2020) reviewed protected and verifiable blockchain-based data storage for the internet of things. The data was sent from the cluster heads to the BS in this configuration. Therefore, BS stores all the critical parameters on a distributed blockchain, and the substantial data is sent to clouds. All certificates of rogue nodes that have been revoked are removed from the blockchain by BS. The detection accuracy, certification latency, computational, and communicational overheads of the proposed approach were all analyzed. The simulation results, analysis, and security verification all point to the suggested method began an improvement above the current state of the art [8].

Yazdinejad, A et al. (2019) focused on the decentralized verification for the energy-savvy ocean IoT using blockchain. They advocate for blockchain technology to be used in an IoUT decentralized authentication system since it was secure, open, and uses little power. Our experimental find demonstrate that the suggested strategy was feasible on underwater devices with constrained resources. When compared to traditional authentication approaches, the suggested model's decentralised authentication in a cluster network significantly reduces device energy usage by 74.63%. In addition, the suggested strategy reduces total delivery time by more than 41.9% while simultaneously increasing it by 21.6% [9].

Hong, S et al. (2020) did research on the sensor node authentication in the IoT using peer-to-peer networking and blockchain technology.The IoT was a network of disparate computing devices and infrastructure. Heterogeneous terminals, networks, and applications were all required to function together seamlessly. As the IoT platform opens up, they would speed up. This would lead to an increase in both technical and administrative security risks in the IoT ecosystem. The protocols used by sensor nodes should be efficient and safe. Different Internet of Things gadgets serve different functions, thus an operating system with a powerful chipset and a secure authentication process may be necessary for some of them. However, in order to switch the lights on or off Simple IoT devices may not even have an operating system installed and may instead rely on a low-performance chipset? An insecure and underpowered device was one that does not use encryption protocols or certificates [10].

Almadhoun, R et al. (2018) considered the blockchain-enabled fog nodes, an IoT authentication scheme was developed. To authenticate users for access to IoT devices, they propose a technique where blockchain-enabled fog nodes interact with Ethereum smart contracts. In order to make the system scalable, fog nodes were used to alleviate the burden of authentication and blockchain communication on the IoT devices. Key topics related to security analysis, functionality, testing, and implementation of the smart contracts was discussed, and the components, architecture, and design of the system were outlined. Github also had the whole source code for the smart contracts that power the authentication registry, lists, rules, and logic [11].

5. PROBLEM STATEMENT

The relevance of previous research to real-world scenarios has not been adequately examined. Previous studies just scratched the surface of the issue. There is an immediate need to improve the precision and effectiveness of blockchain technology with wireless sensor networks (WSN). In addition, the previous research did not think about how WSN, security, and authentication may be combined. This means that previous research has been unable to effectively implement its results in the context in which it was originally done. The earlier research ignored the vast majority of the phenomenon. The precision and effectiveness of WSN are two aspects that require improvement. In addition, the prospects for improvement that might have been taken advantage of by keeping authentication secure on blockchain-based WSN systems were overlooked in the prior studies.

5.1 Proposed work

To ensure the safety of WSN networks, the blockchain and deep learning integration has been made in current research. Incorporating novel hybrid deep learning for classification of secure and insecure data stored on blockchain based WSN is the focus of this study, with the end goal of bolstering the security of Blockchain based WSN infrastructure.

Deep learning is a subfield of machine learning that involves training artificial neural networks to perform various tasks. These neural networks are composed of layers of interconnected artificial neurons (perceptrons) and are capable of learning complex patterns and representations from data. While deep learning involves many mathematical concepts and equations, one fundamental equation in deep learning is the one for a feedforward neural network's operation, which can be represented as follows:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

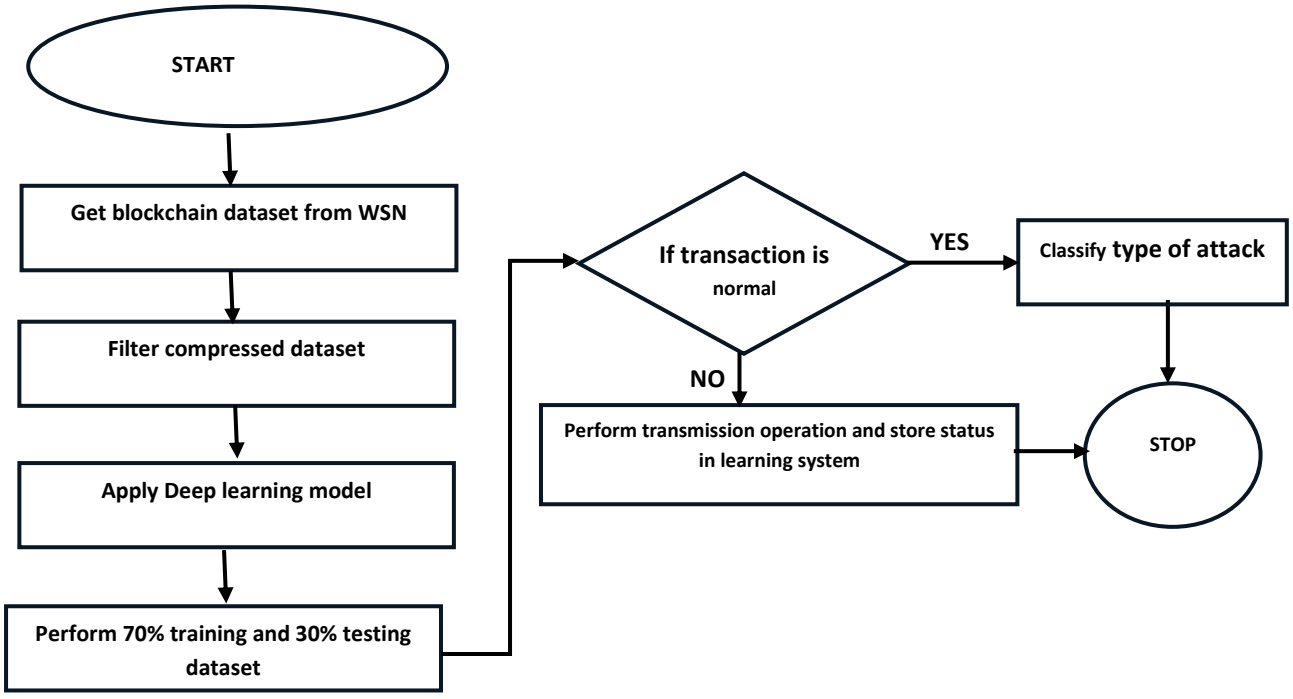

Figure 4 Process flow of Research

5.2 Feedforward Equation (for a single neuron):

The operation of a single artificial neuron in a feedforward neural network can be represented as:

Output (y) = Activation Function (f) [Weighted Sum of Inputs (z)]

Mathematically, it can be expressed as:

$y = f(w * x + b)$

- "y" is the output of the neuron.
- "f" is the activation function (e.g., sigmoid, ReLU, etc.).
- "w" are the weights associated with the connections between the inputs and the neuron.
- "x" are the inputs.
- "b" is the bias term.

5.3Feedforward Equation (for a neural network layer):

When considering a layer of neurons in a neural network, the equation is similar, but applied to each neuron in the layer. The output of a layer can be expressed as:

Output (Y) = Activation Function (f) [Weighted Sum of Inputs (Z)]

Mathematically:

$Y = f(W * X + B)$

- "Y" is the output of the layer (a vector of outputs from all neurons in the layer).
- "f" is the activation function applied element-wise.
- "W" is the weight matrix for the layer.
- "X" is the input matrix (each row corresponds to one input example).
- "B" is the bias vector.

Backpropagation Equation:

Deep learning networks are trained using an optimization algorithm called backpropagation, which involves computing gradients to update the network's weights. The key equation in backpropagation is the chain rule of calculus, which is used to compute the gradients of the loss function with respect to the network's parameters. The specific equations for backpropagation can vary depending on the architecture and loss function used in the network.

These are some of the foundational equations in deep learning, but the field is vast and complex, with many more specialized equations and concepts depending on the specific type of neural network (e.g., convolutional neural networks, recurrent neural networks) and the task (e.g., classification, regression, natural language processing).

Accuracy, precision, and recall are common metrics used in machine learning and classification tasks to evaluate the performance of a model. These metrics are particularly important in binary classification problems (problems with two classes: positive and negative). Here are the mathematical equations for each of these metrics:

Accuracy (ACC):

Accuracy measures the overall correctness of a classification model and is the ratio of correct predictions to the total number of predictions.

Mathematical Equation:

$ACC = (TP + TN) / (TP + TN + FP + FN)$

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

- TP: True Positives (correctly predicted positive samples)
- TN: True Negatives (correctly predicted negative samples)
- FP: False Positives (negative samples incorrectly classified as positive)
- FN: False Negatives (positive samples incorrectly classified as negative)

5.4 Precision (also called Positive Predictive Value):

Precision measures how many of the positive predictions made by the model were actually correct. It's a measure of the model's ability to avoid false positives.

Mathematical Equation:

Precision = TP / (TP + FP)
- TP: True Positives
- FP: False Positives

5.5 Recall (also called Sensitivity or True Positive Rate):

Recall measures how many of the actual positive samples were correctly identified by the model. It's a measure of the model's ability to avoid false negatives.

Mathematical Equation:

Recall = TP / (TP + FN)

- TP: True Positives
- FN: False Negatives

These metrics are essential for evaluating the performance of a binary classification model. Depending on the specific problem and the balance between the importance of precision and recall, you may need to optimize your model for one metric over the other. For example, in medical diagnosis, recall (minimizing false negatives) might be more critical, while in spam email classification, precision (minimizing false positives) could be more important. In some cases, a trade-off between precision and recall is necessary.

6. F1-SCORE

The F1 score is a metric that combines both precision and recall into a single value, providing a balance between these two metrics. It's particularly useful when you want to assess a model's performance in situations where you need to find a balance between minimizing false positives (precision) and false negatives (recall). The F1 score is the harmonic mean of precision and recall and is calculated using the following mathematical equation:

F1 Score = 2 * (Precision * Recall) / (Precision + Recall)

Where:
- Precision is the precision of the model (the number of true positives divided by the sum of true positives and false positives).
- Recall is the recall of the model (the number of true positives divided by the sum of true positives and false negatives).

The F1 score ranges from 0 to 1, with 1 being the best possible F1 score, indicating perfect precision and recall. A higher F1 score suggests a better balance between precision and recall, making it a valuable metric for evaluating the performance of a binary classification model.

6.1 Result and discussion

There is attacks classification with and without optimization. Research is considered two categories such as Secure and insecure that are stored on blockchain based WSN.

Confusion matrix during attack classification without optimization

Table 1 Confusion matrix during attack classification without optimization

	Secure	Insecure
Secure	954	51
Insecure	46	949

Result
TP: 1903
Overall Accuracy: 95.15%

Table 2 Accuracy without optimization

Class	Accuracy	Precision	Recall	F1 Score
1	95.4%	94.93%	95.4%	95.164%
2	94.9%	95.38%	94.9%	95.139%

Confusion matrix during attack classification without optimization

Table 3 Confusion matrix during attack classification with optimization

	Secure	Insecure
Secure	971	32
Insecure	29	968

Result
TP: 1939
Overall Accuracy: 96.95%

Table 4 Accuracy with optimization

Class	Accuracy	Precision	Recall	F1 Score
1	97.1%	96.81%	97.1%	96.955%
2	96.8%	97.09%	96.8%	96.945%

Comparison Analysis of Parameters
ACCURACY
Table 5 shows the outcomes of each class's inventory of the quality of finished work and the priority of future assignments. Data that has been filtered has been proved to be more accurate than the original data that has not been filtered.

Table 5 Comparison of accuracy

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

Class	without optimization	with optimization
1	95.4%	97.1%
2	94.9%	96.8%

Using the information in *table 5*, we can now compare the filtered and unfiltered datasets to demonstrate the improved accuracy of the filtered version in *figure 4*.

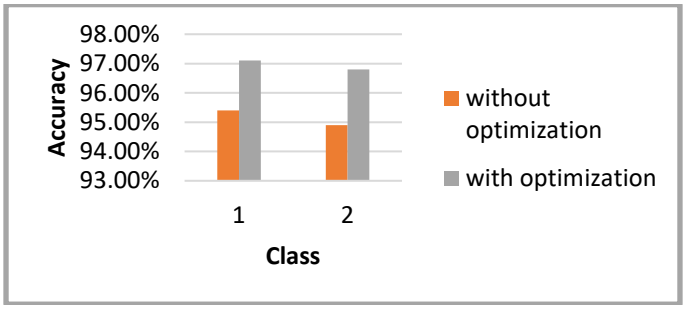

Figure 4 Comparison of accuracy

7. RECALL VALUE

Table 7 displays the results of comparing the recall values of the existing work with the proposed work for classes 1, and 2. One difference between the optimized and non-optimized datasets is shown in the Recall value.

Table 7 Comparison of Recall value

Class	without optimization	with optimization
1	95.4%	97.1%
2	94.9%	96.8%

Taking into account the data in *table 7*, we can see how the optimized model performs in terms of recall by comparing it to the non-optimized in picture 6.

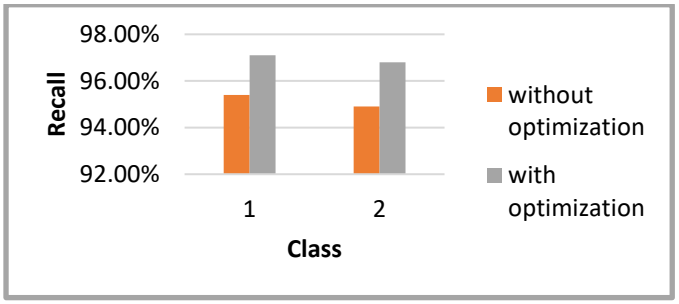

Figure 6 Comparison of recall value

Table 8 displays the F1-scores of completed and planned projects in each of the four classes. The F1-Score of the filtered dataset improves over the unfiltered one.

7.1 F1- SCORE

Table 8 Comparison of F1-Score

Class	without optimization	with optimization
1	95.164%	96.955%
2	95.139%	96.945%

Figure 7 was created based on data in *table 8* to demonstrate the difference between the filtered and unfiltered F1-scores.

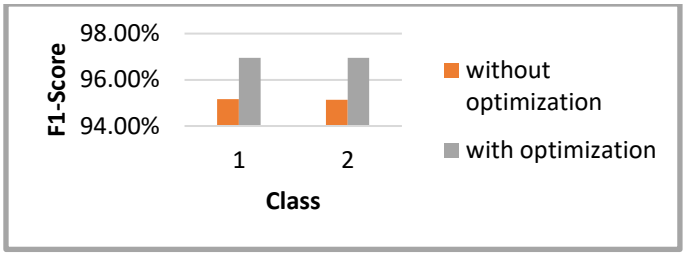

Figure 7 Comparison of f1-score

8. CONCLUSION

Security may be provided via the sophisticated algorithm used by traditional data security techniques such as storing data over blockchain. In contrast to the improve security provided by blockchain over WSN, Deep Learning's training of the data set required preexisting records in order to properly train the computer in order to classify secure and insecure dataset. Hybrid approach used in proposed research has provided better accuracy, precision and recall value as compared to conventional classification mechanism.

8.1 Future Scope

In the future, researchers want to use all of the existing consensus methods, including testing out new digital signature algorithms. Due to the shortcomings of the present authentication methods in the WSN, it is emphasized that blockchain technology be used there. Blockchain has the potential to revolutionize WSN, but there are a number of challenges that must be addressed before it can be used. However, blockchain demands a lot of processing power and energy, and the WSN has limited capacity nodes. The blocks on the blockchain will need more and more room as the number of executed transactions increases. While this is a step in the right direction, more has to be done before WSN applications can take use of the extremely secure properties of blockchain technology. For this reason, a new blockchain-based authentication mechanism tailored to secure WSN applications has been developed. Analyses of the proposed protocol's security and efficiency were positive. This study indicates not only a high degree of security but also efficiency in terms of latency, energy, and memory use. In the future, scientists want to try out other digital signature algorithms and use different types of agreement mechanisms.

REFERENCES

[1] Ghorashi, S.M.; Rastegar, M.; Senemmar, S; Seifi, A.R. Optimal design of reward-penalty demand response programs in smart power grids. Sustainable Cities and Society 2020, Volume 60, pp. 102150.

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 1 | Pages 23-31 | ISSN XXXX-XXXX

[2] Abdel-Basset, M.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Energy-net: a deep learning approach for smart energy management in IoT-based smart cities. IEEE Internet of Things Journal 2021, Volume 8, No 15, pp. 12422-12435.

[3] Huang, C.; Zappone, A.; Alexandropoulos, G.C.; Debbah, M.; Yuen, C. Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE transactions on wireless communications 2019, Volume 18, No 8, pp. 4157-4170.

[4] Abdel-Basset, M.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Energy-net: a deep learning approach for smart energy management in iot-based smart cities. IEEE Internet of Things Journal 2021, Volume 8, No 15, pp. 12422-12435.

[5] Antonopoulos, I.; Robu, V.; Couraud, B.; Kirli, D.; Norbu, S.; Kiprakis, A.; Flynn, D.; Elizondo-Gonzalez, S.; Wattam, S. Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review. Renewable and Sustainable Energy Reviews 2020, Volume 130, pp. 109899.

[6] Merabet, G.H.; Essaaidi, M.; Haddou, M.B.; Qolomany, B.; Qadir, J.; Anan, M.; Al-Fuqaha, A.; Abid, M.R.; Benhaddou, D. Intelligent building control systems for thermal comfort and energy-efficiency: A systematic review of artificial intelligence-assisted techniques. Renewable and Sustainable Energy Reviews 2021, Volume 144, pp. 110969.

[7] Aguilar, J.; Garces-Jimenez, A.; R-moreno, M.D.; García, R. A systematic literature review on the use of artificial intelligence in energy self-management in smart buildings. Renewable and Sustainable Energy Reviews 2021, Volume 151, pp. 111530.

[8] Kathirgamanathan, A.; De Rosa, M.; Mangina, E. and Finn, D.P. Data-driven predictive control for unlocking building energy flexibility: A review. Renewable and Sustainable Energy Reviews 2021, Volume 135, pp. 110120.

[9] Sun, L.; You, F. Machine learning and data-driven techniques for the control of smart power generation systems: An uncertainty handling perspective. Engineering 2021, Volume 7, No 9, pp. 1239-1247.

[10] Erciyes, K. Graph-Theoretical Analysis of Biological Networks: A Survey. Computation 2023, Volume 11, No 10, pp. 188.

[11] Zervoudakis, K.; Tsafarakis, S. A mayfly optimization algorithm. Computers & Industrial Engineering 2020, Volume 145, pp. 106559.