Design of a Hybrid Authentication Technique for User and Device Authentication for an integrated IOT environment using Blockchain Authentication and Artificial Intelligence

Ashish Dibouliya

Principal Architect – Data, Connecticut, USA

***

Abstract - *Attacks against Internet of Things (IoT) devices have increased dramatically in recent years. Attacks on vital internet infrastructure systems have been carried out by cyber thieves using hacked IoT devices. Information security researchers are under increasing pressure to provide new tactics and solutions to protect susceptible devices at all levels following recent assaults. When it comes to home networks, malevolent actors don't care about the smart devices that are part of them. National and global governments are placing a high value on securing critical IoT networks like the electrical grid and water distribution systems. Many different technologies are being applied to the problem of Internet of Things security. These include blockchain, AI, and edge/fog computing (IoT). Authentication and authorization are two legs of the CIA's crucial triad of components. However, due to the scale of IoT networks and the limited resources of devices, standard authentication and authorization mechanisms are unsuitable for handling security. We employ blockchain technology as a lightweight and straightforward authentication solution for IoT devices. The use of artificial intelligence (AI) to aid in decision-making and carry out predictive analytics in a wide variety of contexts is gaining popularity. In recent years, blockchain (a peer-to-peer distributed system) has also been used to enable AI applications, such as secure data sharing (for model training), data privacy, trustworthy AI decision making, and decentralized AI. The purpose of this effort is to create a hybrid authentication technique based on Blockchain authentication and AI for user and device authentication in a fully interconnected IOT setting.*

Keywords: *IOT (Internet of Things), WSN (Wireless Sensor Networks), Blockchain Authentication, Artificial Intelligence, Hybrid Authentication*

1. INTRODUCTION

The concept of the Internet of Things (IoT) is rapidly growing and gaining popularity. Many of our regular tasks and routines would be impossible without the Internet of Things. New IoT applications in areas including smart homes, smart healthcare, smart cities, industry 4.0, wireless sensor networks (WSN), and smart farming have the potential to introduce and advance the concept of a smart world. Security measures at several layers, along with the capacity to analyze and regulate all data and information, are essential for the platforms, networks, devices1, and applications that make up the Internet of Things (IoT) ecosystem. The devices can be easily compromised, leaving users open to identity theft and meddling with their data.

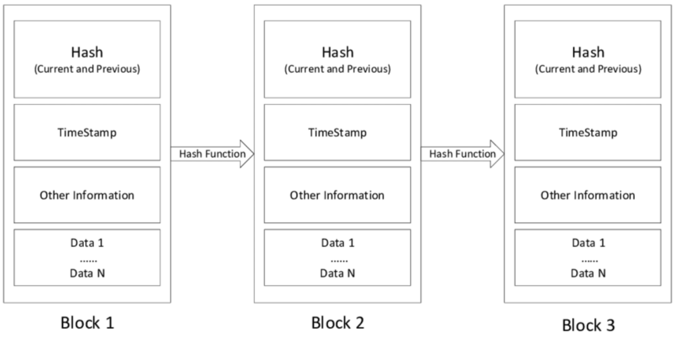


Figure: 1 Basic Blockchain Structure

The ledger must be generated and maintained by each node in the blockchain ecosystem. To participate, a participant must be able to read and write transactions. There are two categories of participants: read-only and read-write. To put it another way, miners can add transactions to the chain as unique nodes. An established technology, blockchain holds a lot of promise. It is regarded as a fundamental approach in a decentralized network environment since it is distributed, decentralized, and unchanging. For the blockchain network's peers to accept a block, miners must complete proof of work (PoW). Figure 1 depicts the blockchain's basic structure. For securing the Internet of Things (IoT), Blockchain has been hailed as an ideal option. To ensure the safety of the IoT ecosystem, we have also benefited from this technology. It is our primary purpose in this research project to provide an authentication system based on the Ethereum Blockchain, which is a public blockchain and provides distributed and decentralized security for IoT devices. Using this method, users and their gadgets may communicate in a secure environment. There are three sections in which the document is broken down: 1st section includes introduction part of the paper. Second, there is a section called Related Work that provides an overview of the blockchain and includes work done by other authors to secure IoT with blockchain. Third is the Proposed Technique, which includes the results and discussion of the proposed method, and finally Section V is the Conclusion.

1.1 Internet of things paradigm

IoT is now a reality that pervades many aspects of our life, and it is only going to becoming more prevalent in the future. Although IoT was formerly viewed as a science fiction concept, it has now become a reality thanks to the work of several researchers who see it as one of the most significant technical shifts of the twenty-first century. A single linked thing per person was achieved in 2008, and current estimates place the number at roughly 26 smart objects per person by 2020. There are still many challenges that need to be overcome before the Internet of Things can be used to its full potential. These challenges include but are not limited to computing constraints imposed by Internet of Things (IoT) devices; heterogeneity; identification; power supply; data storage/processing; among other things. Security and privacy are two of the most pressing issues, considering the widespread use of smart devices in everyday life. IoT security solutions aren't applicable in general because of the restrictions of IoT components, which have minimal capabilities in both energy and processing resources.

As a result, they cannot implement elaborate schemes supporting security. Unfortunately, this makes things even more difficult. Most prevalent IoT exploits, and vulnerabilities have been documented by the OWASP Internet of Things Project.

1.2 IoT and Machine learning algorithms

Most devices that participate on the internet of things are autonomous and have modest power requirements. These nodes can collect data, act based on that data, and communicate with one another and with other entities thanks to the use of sensors, actuators, and even the Cloud. When the complexity of the algorithms became too difficult to manage, attention turned from artificial intelligence (AI) to machine learning (ML). Machine learning methods are used in numerous modern contexts, from statistical analysis and prediction to practical tasks like speech recognition and fraud detection. Algorithms and methods used in machine learning have been impacted by many disciplines, including mathematics, neuroscience, statistics, and computer science. To test an algorithm's ability to learn from data, it is common to split the development of the algorithm into two distinct phases: the training phase and the verification phase. Most today's machine learning algorithms fall under the categories of unsupervised, supervised, and reinforcement learning. For the first-class training phase to be successful, a labelled data set is required so that the studied relationships can be represented. In contrast to the first type, the input/output pairings for the unsupervised learning techniques are not provided. The primary focus of this activity is on locating the links between the various data points. The third type, online learning, describes situations in which an agent acquires knowledge about how to behave by engaging in trial-and-error interactions with an interactive environment.

1.3 Objective of Paper

Design and development of an authentication technique which employees hybrid algorithms/techniques such as Blockchain Authentication and Artificial Intelligence, for seamless user as well as device authentication in an IOT network.

2. LITERATURE SURVEY

Achraf Fayad et. All (2019) Numerous studies have been done to propose novel methods and systems for ensuring the authentication of IoT devices. Many existing efforts do not meet all of the IoT's objectives, such as permitting the mobility of nodes or guaranteeing scalability through decentralised techniques or making it easy to integrate new devices and services. The authors of this paper put up a simple way of authentication in this situation. Using a blockchain, which is entirely decentralised, is at the heart of our answer to this problem. As a result, it fulfils all of the previously described conditions. Real-world implementations of our method were used to test the validity of our findings. It was evident from the results that it was low in weight. [1]

Aissam Outchkoucht et. All (2017) Even as the mechanisms for actuation, communication, and control improve and become more widespread, the risks they pose to user trust and the Internet of Things as a whole, when not adequately addressed, are also increasing in sophistication and pervasiveness. This investigation has centered on the IoT (Internet of Things). It proposed a framework with the intention of fixing two issues: I those that arise from using a centralized design, and (ii) the need to transmit the administration of access control from a central body to the nodes of the network. Indeed, the limited devices of the Internet of Things do not have the computational resources or data storage space required to support a decentralized access control system. The sheer number of connected smart devices can be overwhelming in an IoT setting, posing a number of regulatory issues related to regulating user access. As a result, security officers and managers often resort to enforcing "static policies," in which all security and access control rules are written by a single person. [2]

Soumyashree S. Panda et. All (2019) The Internet of Things (IoT) and its many uses have become an integral part of our everyday lives. Without the need for human intervention, a number of smart devices can interact with one other. To participate in an autonomous system, only genuine entities should be able to participate. As a result, this study proposes an IoT system authentication scheme. Blockchain is the decentralised ledger technology that would be used in the proposed system, not a central authority. [3]

Khadija Fazal et. All (2020) Authenticated users must be able to access and retrieve data from each device. Access to these gadgets and the communications they provide should be safe in most instances. IoT security is a key roadblock to widespread adoption and implementation of the technology, for a variety of reasons, including the fact that it is extremely vulnerable to cyberattacks. Authors present a blockchain-based Ethereum authentication system for constructing safe zones in the internet of things. Various IoT settings, services, and situations can benefit from the authors' proposed strategy. We can be confident in the security of our system because we are using a public form of Blockchain. To test the suggested approach, we want to write a smart contract in solidity using the Remix IDE and analyse its performance in terms of cost and time. [4]

Dr. Sakthi Kumaresh et. All (2021) In this article, a Decentralized Artificial Intelligence-enabled Blockchain network is implemented using the confluence of AI and Blockchain technology (DAIBCN). The proposed DAIBC method uses a decision tree model to automatically identify miner nodes. There is less requirement for miner nodes to perform complex hash functions in order to be eligible for reward. The testing findings reveal that the suggested AI-enabled approach saves a significant amount of energy and also reduces the time it takes to complete a transaction because the node selection is done automatically. [5]

Praveen Kumar Kollu et. All (2021) Blockhain development has spurred continuing study in a variety of theoretical and functional areas. Decentralization, identity, and trust are three of today's most pressing technological issues, and the blockchain is widely seen as a promising answer even as it is still in its infancy. When it comes to finding the best way to store and access cloud data, the groundbreaking blockchain is an invaluable resource. This article examines the potential of blockchain technology to defend cloud computing. A cloud computing data security mechanism is also presented in this paper. This application uses smart contracts and permission lists to secure data security. [6]

Shanshan Zhao et. All (2019) Data is generated, collected, processed, sent, and stored by several organisations in an IIoT ecosystem. Blockchaining both IIoT entities and business processes is highly sought after by the sectors. The Internet of Things (IIoT) is predicted to be widely implemented in sectors as a result of fast technological advancements and new business models. In this article, we've looked at blockchain and IIoT integration from an industrial standpoint. Introduced is a blockchain-enabled architecture for the Internet of Things (IoT). The most important applications and issues are covered. Blockchain-enabled IIoT research issues and potential trends were also examined by the authors. [7]

Muhammad Tahir et. All (2020) Authentication, privacy, chaos, mining, and administration are just a few of the issues that the growing IoT market and the Blockchain ecosystem are creating. In IoT applications, mutual authentication is essential because it gives security to users and assures the validity of data and protects their privacy. The mutual authentication of IoT devices has been separated into distinct classes based on the authentication and assessment methodologies. A innovative approach for mutual authentication and authorisation is presented in this work by the authors. Distributed joint conditional probability and the selection of random numbers are used to establish robustness in the proposed framework. The performance assessment and results analysis reveal that the suggested framework achieves better security strength, fewer communication overhead costs, and consumes less time in processing data together with increased security. [8]

Dr Mohd Javaid et. All (2021) In addition to ensuring the safety of all communications between the many interconnected smart devices, the blockchain also keeps a permanent record of every single message ever sent. Individuals' identities could also be protected via blockchain technology. Due to its deceptive nature, this technology enables its users to establish a safe and dependable online persona. A Blockchain identity might be used for anything from a single click to accessing a whole suite of applications and services or even forging digital signatures. Blockchain could be useful for SMEs and suppliers as it offers a secure, high-quality transactional data source. Furthermore, a shop must guarantee that all of its products are of uniform quality. [9]

Bhabendu K. Mohanta et. All (2019) The Internet of Things (or IoT) is a relatively new concept. Smart homes, smart cities, smart transportation, and smart healthcare systems are just a few examples of how IoT is enhancing human well-being in a variety of contexts. Real-time monitoring and control are available in all circumstances. To test the efficacy of the DecAuth (Decentralized Authentication) system, this paper proposes a Blockchain-based ethereum platform implementation. An IoT device may be authenticated in a decentralised manner, according to the experimental results. Also, according to the study, the suggested system is impenetrable by the currently known assaults. [10]

Jesse Yli-Huumo et. All (2016) The Bitcoin cryptocurrency is powered by blockchain technology. An open ledger of all transactions is maintained in a decentralized setting that is accessible to everyone. Blockchain aims to give its users with complete anonymity, safety, privacy, and transparency. However, these characteristics pose several technological issues and constraints that must be addressed. Authors used the systematic mapping study approach to map all relevant studies on Blockchain technology to better grasp the present state of the field. The study's main objective was to map out the existing state and future directions of blockchain technology. Aside from the technical viewpoint, writers in this study did not offer viewpoints on economics, law, business, or regulation. From scientific databases, 41 primary publications were retrieved and examined by the authors. [11]

3. METHODOLOGY

3.1 Proposed Work Block Diagram

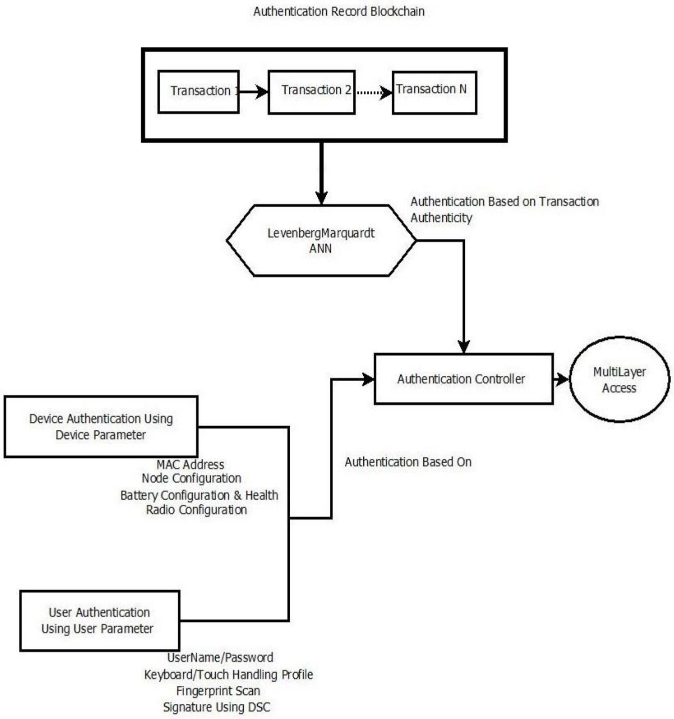

Authentication Record Blockchain
Transaction 1
Transaction 2
Transaction N
LevenbergMarquardt ANN
Authentication Based on Transaction Authenticity
Authentication Controller
MultiLayer Access
Device Authentication Using Device Parameter
MAC Address
Node Configuration
Battery Configuration & Health
Radio Configuration
Authentication Based On
User Authentication Using User Parameter
UserName/Password
Keyboard/Touch Handling Profile
Fingerprint Scan
Signature Using DSC

Figure: 3.1 Proposed Work Block Diagram

The proposed system is aimed for seamless authentication of User(s) & Device(s) in IOT-WSN Network's, the system employs a block – chain of user/device authentication entries, which is used to train a Function Fitting Neural Network, which is used to ascertain the authenticity of new block - chain entry for user/device authentication, in form of a transaction authenticity score.

Apart from block - chain based login access; secondary authentication is provided based User and Device parameters listed below. The user/device parameters are used to train another pattern matching neural network, which is used to provide User/Device Authentication Score.

Block-Chain based authentication score is combined with User/Device authentication score using custom machine intelligence to generate final authentication score, which is used to provide multi-layer access to various services and resources hosted by the IOT – WSN Network.

About LEVENBERG-MARQUARDT

To calculate the minimum of a function (linear or nonlinear) over a space of parameters, the well-known Levenberg-Marquardt algorithm (LMA) is often employed. A function, such as a quadratic, is used internally to mimic a reliable portion of the goal function. Once a good match is established, the trusted area grows to include the new addition. The Levenberg-Marquardt methodology is sensitive to the initial beginning parameters, as is the case with many numerical algorithms. This article describes the training and testing phases of the Levenberg-Marquardt algorithm for learning artificial neural networks.

Why LEVENBERG-MARQUARDT:

The created LM-ANN model is more sensitive for prediction of the inflows when the statistics of the long-term and seasonal-term outputs are compared. Further, the speed and reliability of the LM-ANN technique make it applicable to the modelling of a wide range of hydrological factors. For a given collection of training data, the Levenberg Marquardt (LM) training function achieved the best performance (the smallest MSE). Levenberg Marquardt is found to be the most effective predictive algorithm through extensive testing.

Key Benefits of LEVENBERG-MARQUARDT Algorithm:

1. The LM algorithm is more robust and has more stable convergence than thee GN algorithm
2. This algorithm is mostly used for training small and medium sized problems in ANN.
3. The advantage of the approach is that, once the network is trained, it allows instantaneous evaluation of solutions at any desired number of points; thus, spending little computing time.
4. Levenberg-Marquardt algorithm gives the best results with high performance.
5. The Levenberg-Marquardt (LM) gradient descent algorithm is used extensively for the training of Artificial Neural Networks (ANN).
6. The Levenberg–Marquardt algorithm provides a numerical solution to the problem of minimizing a (generally nonlinear) function.
7. The LEVENBERG-MARQUARDT method is a single-shot method which attempts to find the local fit-statistic minimum nearest to the starting point.

How LEVENBERG-MARQUARDT Helps

In the proposed work Levenberg–Marquardt algorithm Used for train artificial neural network and process some functions than some mathematical calculation will be perform then train function, then plot error and performance plot and calculated estimated distance with respect or transmit power. if any node tries to establish connection in our network, if this is in our range then our access controller provided true key for establish connection with some leniency otherwise if this is in outside the range then access controller provided fake random key for privacy.

3.1.1 User & Device Parameters Used

User Parameters

S.No	Parameter Name	Narration
1.	User Name/Password	Primary Access Control & User Identification
2.	Keyboard/Touch Handling Profile	2nd Factor Authenticator Using Comparison of Keyboard/Touch Handling With Previously Known History
3.	Fingerprint Scan	2nd Factor Authenticator Using Biometric – Fingerprint Scan Using Minutiae Extraction &Euclidian Distance Computation
4.	Signature Using DSC	2nd Factor Authentication Using Digital Signature Certificate Provided By Trusted Authority Such As CCA In India

Table: **3.1** User Parameters

Device Parameters

S.No	Parameter Name	Narration
1.	MAC Address	Primary Device Identifier, Using Unique Machine Address Used For Direct Node Address Usage or Referenced Usage Such As IP Address Based Redirection
2.	Node Configuration	2nd Factor Authenticator Using Computing Configuration of The Device Such As Processor Speed, Number of Cores, RAM, Flash ROM, Architecture Etc
3.	Battery Configuration & Health	2nd Factor Authenticator Using Battery Configuration, Voltage, mAh, Technology,No. of Banks Etc Along With Battery Health Monitoring
4.	Radio Configuration	2nd Factor Authenticator Using Wireless/Radio Configuration of The Node/Device Such As Transmit power, Receive Sensitivity, Noise Floor Etc

Table: 3.2 Device Parameters

3.2 Trusted Node RF Ranging Based Location/Distance Approximation

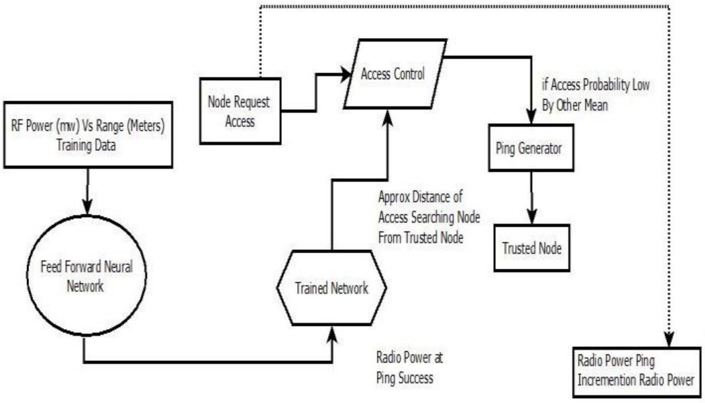
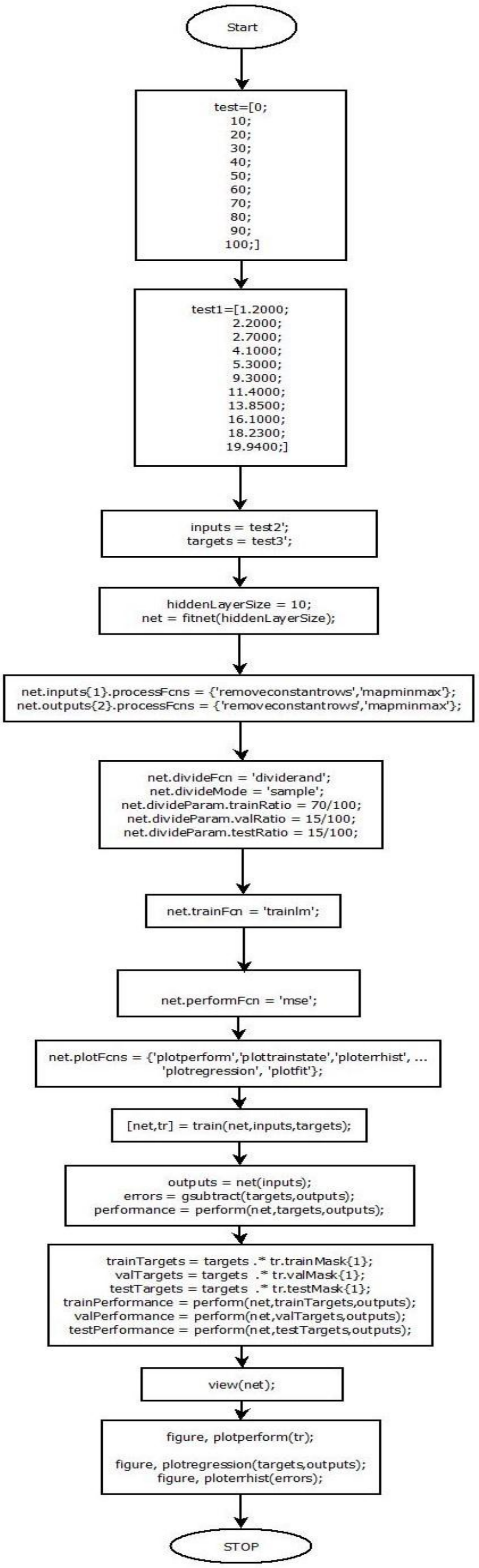

RF Power (mw) Vs Range (Meters) Training Data
Node Request Access
Access Control
if Access Probability Low By Other Mean
Ping Generator
Approx Distance of Access Searching Node From Trusted Node
Trusted Node
Feed Forward Neural Network
Trained Network
Radio Power at Ping Success
Radio Power Ping Incremention Radio Power

Figure: 3.2 Trusted Node RF Ranging Based Location/Distance Approximation

Apart from the authentication path described above, another method of improving authentication score is provided, for User/Device denied access by marginal difference in authentication score, by verification of their physical/geographic proximity to the trusted/central node using a novel technique developed using Artificial Intelligence & slowly increasing Transmit Distance by varying the Radio Power using Transmit Power Estimation ANN, until ping is replied by the User/Device requesting access. After each ping, the pin generator increases the power by a certain amount until a node connects. Once a node does connect, the trained network calculates its distance from an access controller and provides a key and some leniency in access. The access controller will provide a false (fake) key if the neural networks calculated range is greater than the coverage range. This is how we'll verify the authenticity.

3.3 Artificial Neural Network Flow Chart



```
test=[0;
10;
20;
30;
40;
50;
60;
70;
80;
90;
100;]
```

```
test1=[1.2000;
2.2000;
2.7000;
4.1000;
5.3000;
9.3000;
11.4000;
13.8500;
16.1000;
18.2300;
19.9400;]
```

```
inputs = test2';
targets = test3';
```

```
hiddenLayerSize = 10;
net = fitnet(hiddenLayerSize);
```

```
net.inputs{1}.processFcns = {'removeconstantrows','mapminmax'};
net.outputs{2}.processFcns = {'removeconstantrows','mapminmax'};
```

```
net.divideFcn = 'dividerand';
net.divideMode = 'sample';
net.divideParam.trainRatio = 70/100;
net.divideParam.valRatio = 15/100;
net.divideParam.testRatio = 15/100;
```

```
net.trainFcn = 'trainlm';
```

```
net.performFcn = 'mse';
```

```
net.plotFcns = {'plotperform','plottrainstate','ploterrhist', ...
'plotregression', 'plotfit'};
```

```
[net,tr] = train(net,inputs,targets);
```

```
outputs = net(inputs);
errors = gsubtract(targets,outputs);
performance = perform(net,targets,outputs);
```

```
trainTargets = targets .* tr.trainMask{1};
valTargets = targets .* tr.valMask{1};
testTargets = targets .* tr.testMask{1};
trainPerformance = perform(net,trainTargets,outputs);
valPerformance = perform(net,valTargets,outputs);
testPerformance = perform(net,testTargets,outputs);
```

```
view(net);
```

```
figure, plotperform(tr);

figure, plotregression(targets,outputs);
figure, ploterrhist(errors);
```

Figure: 3.3 Artificial Neural Network Flow Chart

Neural networks are self-learning adaptive systems that use interconnected nodes (sometimes called neurons) in a multi-tiered architecture like the human brain (also known as artificial neural networks). By being fed enough information, a neural network can learn to identify patterns, organize information into categories, and make predictions about the future. The input is broken down into levels of abstraction by a neural network. It may be taught to detect patterns in speech or images, for example, using many samples, just like a human brain. A system's behavior is determined by the way its components are linked together and the weights attached to those links. To achieve the required job, these weights are automatically modified during training based on a predetermined learning rule. In this flow chart we can see 1st our ANN code is start than call to test values then input and targets test values then hidden layer operation perform then process some functions than some mathematical calculation will be perform then train function, then plot error and performance plot after that code will be stop.

4. RESULT

4.1 ANN Results

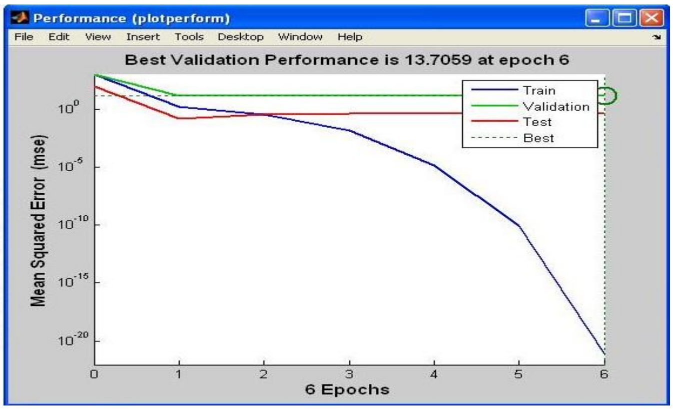


Figure: 4.1 Best Validation Performance Plot

The accompanying diagram depicts the Artificial Neural Network's best validation performance plot. The best, validation, test, and railway lines are all displayed here. Error typically reduces with additional training epochs but may increase on the validation data set if the network begins to overfit the training data. Epochs with low validation errors get the greatest results with the default configuration after a series of six consecutive increases in validation error.

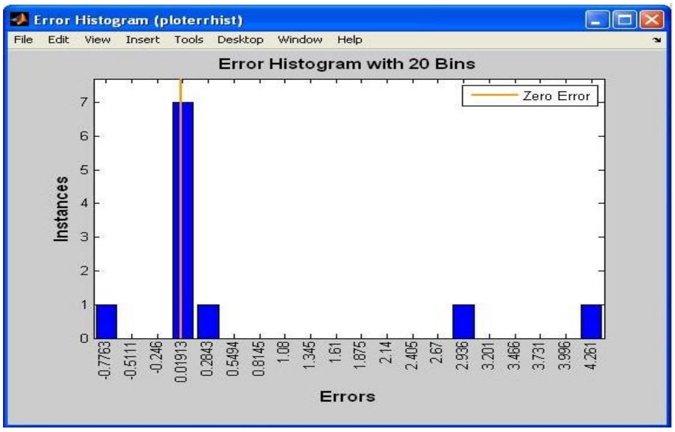


Figure: 4.2 Error Histogram Plot

The error histogram plot produced by our neural network simulation is displayed above. An error histogram is a histogram of the deviations from the desired value, or forecast, that occurred after training a feedforward neural network. Because they indicate how far the projected values deviate from the desired ones, these error numbers can be negative. The number of discrete categories (or "bins") in a bar chart. The histogram is a form of bar chart that displays numerical data by organizing it into discrete buckets. The error bars in the preceding graph range from a high of 0.01913 at 7 instances to a low of 0.2843.

4.2 Estimated Power Results

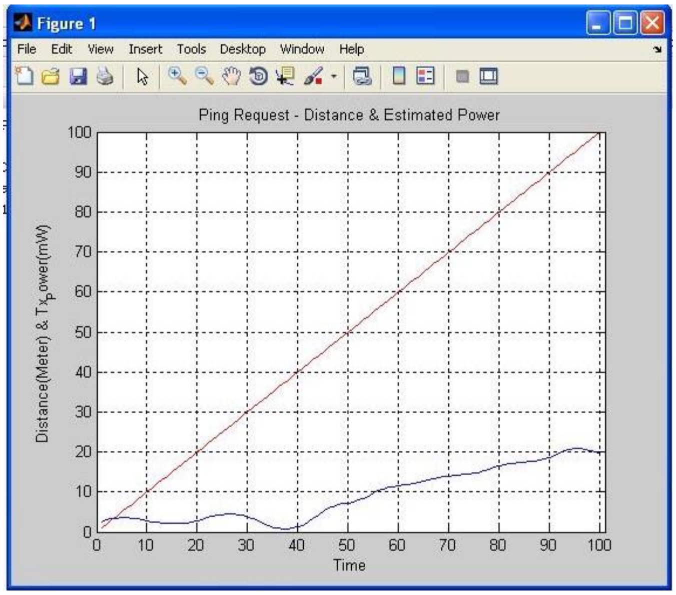
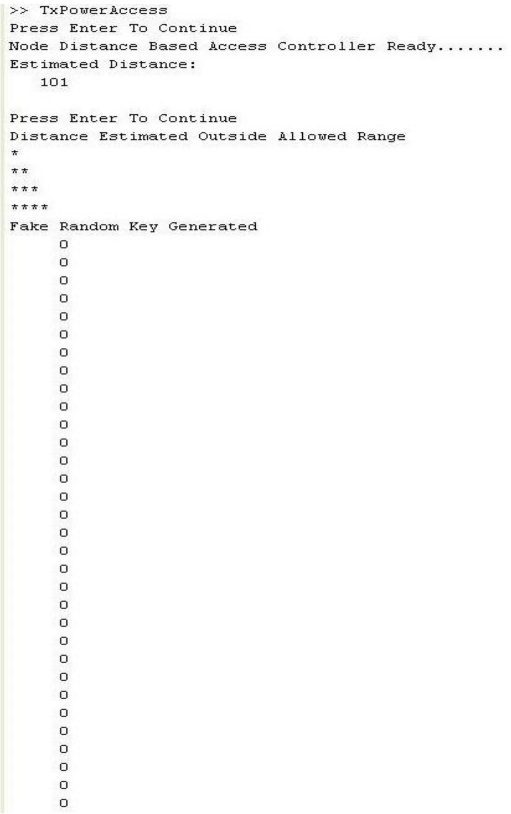


Figure: 4.3 Ping Request- Distance & Estimated Power

The above result is for power estimation based on distance, access controller starts sending ping request at the 0 second, and continuously sent pin with time interval of 10 seconds with increment of some power after each 10 seconds of time interval. At the 0 (zero) meter transmit power estimated is 3 mw and ping is success after 100 seconds. At the distance of 101 meter and power estimated on this distance is 20 mw ping is success. This distance is outside the range of coverage area so there is risk in privacy if connection is established so access controller sent fake random key that is in the form of zero for provide security to network.

S. NO.	Time	Distance	Power
1	0 Sec.	0 meter	3 mw
2	10 Sec.	10 meters	2 mw
3	20 Sec.	20 meters	3 mw
4	30 Sec.	30 meters	4 mw
5	40 Sec.	40 meters	2 mw
6	50 Sec.	50 meters	8 mw
7	60 Sec.	60 meters	11 mw
8	70 Sec.	70 meters	14 mw
9	80 Sec.	80 meters	17 mw
10	90 Sec.	90 meters	19 mw
11	100 Sec.	101 meters	20 mw

Table: 4.1 Ping Request- Distance & Estimated Power



```
>> TxPowerAccess
Press Enter To Continue
Node Distance Based Access Controller Ready.......
Estimated Distance:
   101

Press Enter To Continue
Distance Estimated Outside Allowed Range
*
**
***
****
Fake Random Key Generated
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
```

Figure: 4.4 Fake Random Key Generated

In this above figure we can see ping received at the distance of 101 meter and at this distance transmit power is 20 mw, this range of distance estimated is outside of the allowed range, so access controller generates fake random keys in the form of zeros and provide to node for authentication and privacy of network.

4.3 Node Distance Based Access Controller Result

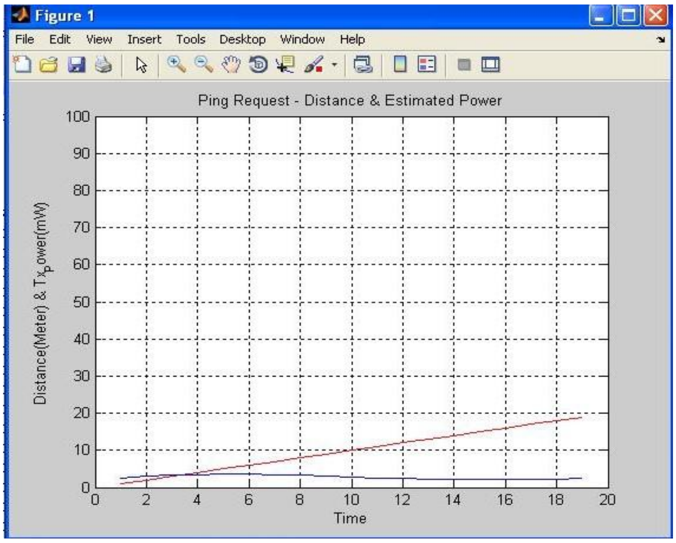
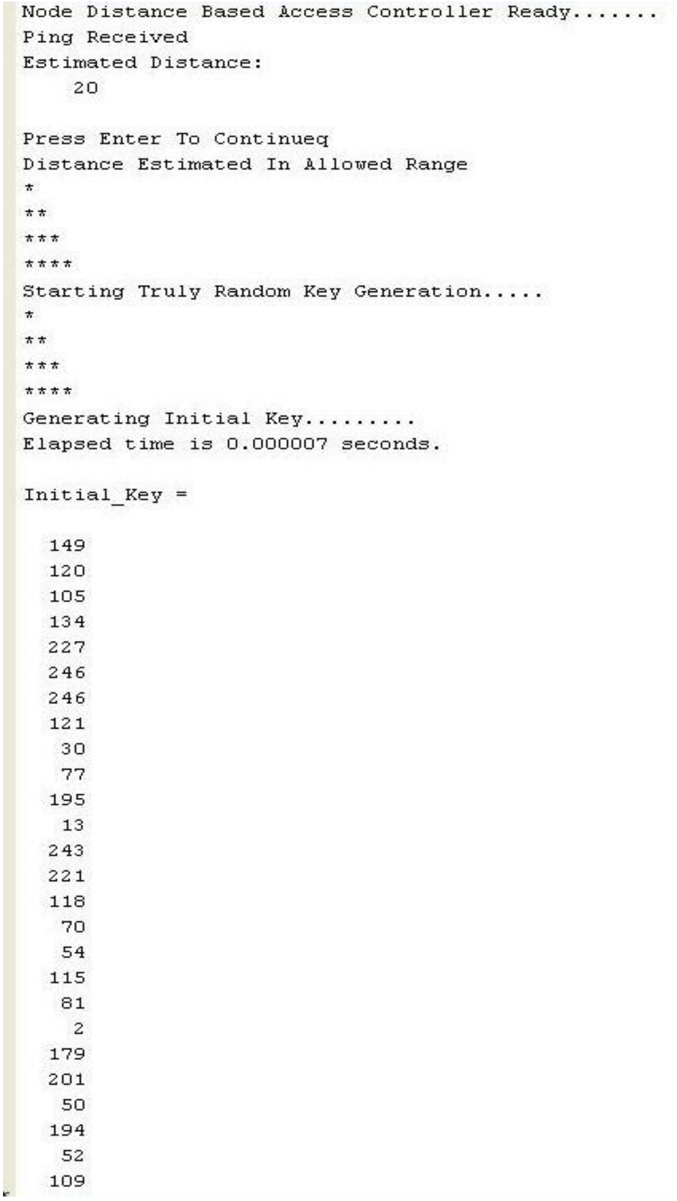


Figure: 4.5 Ping Request – Distance & Estimated Power

Above figure shows distance estimation with power, access controller starts sending ping request with 2mw power, at this power distance estimated by trained network is 1 meter at 1second. Access controller sent ping request continuously with increment of some power, after 19 seconds with 2 mw power estimated distance calculated by trained network is 19 meters at this point ping is success because this range in converge area so access controller provide initial key for establish connection with some leniency in access.

S. NO.	Time	Distance	Power
1	1 Sec.	1 meter	2 mw
2	2 Sec.	2 meters	2.5 mw
3	4 Sec.	4 meters	3 mw
4	6 Sec.	7 meters	3 mw
5	8 Sec.	8 meters	2.5 mw
6	10 Sec.	10 meters	2 mw
7	12 Sec.	12 meters	2 mw
8	14 Sec.	14 meters	2 mw
9	16 Sec.	17 meters	1 mw
10	18 Sec.	18 meters	1 mw
11	19 Sec.	19 meters	2 mw

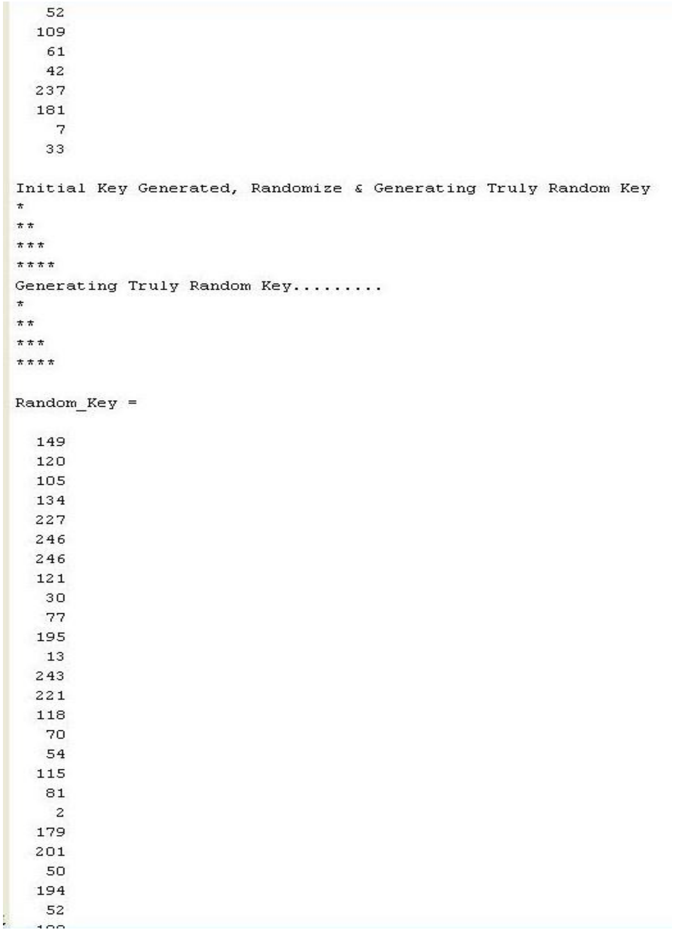
Table: 4.2 Ping Request – Distance & Estimated Power



```
Node Distance Based Access Controller Ready.......
Ping Received
Estimated Distance:
    20

Press Enter To Continueq
Distance Estimated In Allowed Range
*
**
***
****
Starting Truly Random Key Generation.....
*
**
***
****
Generating Initial Key.........
Elapsed time is 0.000007 seconds.

Initial_Key =

   149
   120
   105
   134
   227
   246
   246
   121
    30
    77
   195
    13
   243
   221
   118
    70
    54
   115
    81
     2
   179
   201
    50
   194
    52
   109
```

Figure: 4.6 Initialized Key

In this above figure we can see estimated distance and initialize key. Above figure shows that node is in converge range, so node distance-based access controller is ready for establish connection between node and access controller, because ping is received at distance of 19 meter. So, access controller proved initial key, generated initial key we can also see in above figure.



```
   52
  109
   61
   42
  237
  181
    7
   33

 Initial Key Generated, Randomize & Generating Truly Random Key
 *
 **
 ***
 ****
 Generating Truly Random Key.........
 *
 **
 ***
 ****

 Random_Key =

  149
  120
  105
  134
  227
  246
  246
  121
   30
   77
  195
   13
  243
  221
  118
   70
   54
  115
   81
    2
  179
  201
   50
  194
   52
```

Figure: 4.7 Generated Random Key

In this above figure we can see generated truly random key.

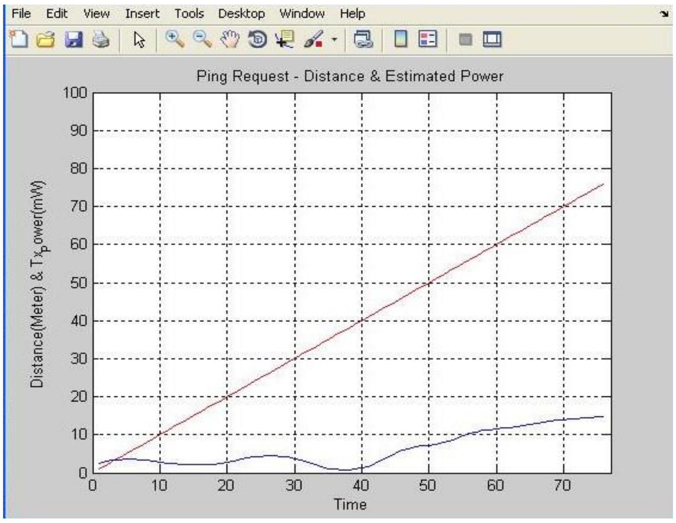
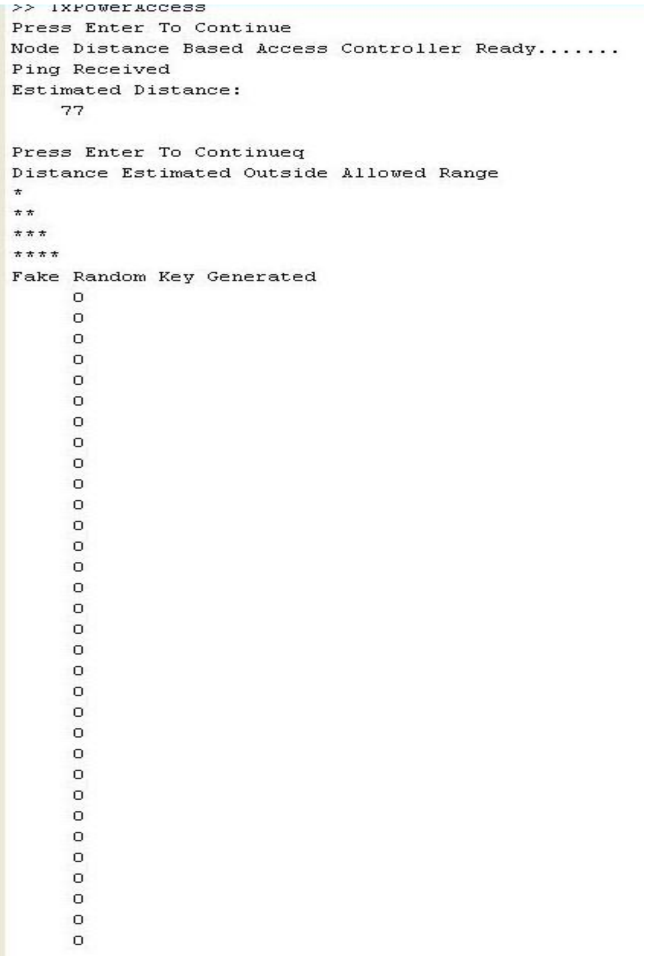


Figure: 4.8 Ping Request- Distance & Estimated Power

The above figure shows distance estimation with power, access controller starts sending ping request with 0 mw power, at this power distance estimated by trained network is 0 meter at when time is 0 second. Access controller sent ping request continuously with increment of some power with the time interval of 10 seconds, after 78 seconds with 15 mw power estimated distance calculated by trained network is 77 meters at this point ping is accept. But this distance is not in converge range, so access controller provides fake key for privacy of network.

S. NO.	Time	Distance	Power
1	0 Sec.	0 meter	3 mw
2	10 Sec.	10 meters	2 mw
3	20 Sec.	20 meters	2 mw
4	30 Sec.	30 meters	4 mw
5	40 Sec.	40 meters	1 mw
6	50 Sec.	50 meters	8 mw
7	60 Sec.	60 meters	12 mw
8	70 Sec.	70 meters	14 mw
9	78 Sec.	77 meters	15 mw

Table: 4.3 Ping Request- Distance & Estimated Power



```
>> TxPowerAccess
Press Enter To Continue
Node Distance Based Access Controller Ready.......
Ping Received
Estimated Distance:
    77

Press Enter To Continueq
Distance Estimated Outside Allowed Range
*
**
***
****
Fake Random Key Generated
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
     0
```

Figure: 4.9 Fake Random Key Generated

In this above figure we can see ping received at the distance of 77 meter and their transmit power is 15 mw, this range of distance estimated is outside of the allowed range, so access controller generates fake random keys in the form of zeros and provide to node for authentication and privacy of network.

5. CONCLUSIONS & FUTURE SCOPE

Conclusion

Blockchain technology is used in the suggested system. Blockchain-based security mechanisms may also be implemented in the real world. The same blockchain architecture allows players to identify each device. The data put into the system is unquestionable and may be used to identify the device that supplied it. IoT applications will benefit greatly from blockchain's ability to provide secure, distributed authentication and authorization of IoT devices. Smart contracts can confirm device message exchanges on the blockchain, making it possible to secure device communication.

IoT protocols can be more secure with the aid of blockchain technology. In the Blockchain, messages sent between devices may be seen as transactions, and smart contracts can be used to verify them. IoT protocols can be more secure with the aid of blockchain technology. The goal proposed work is provided privacy in network based on distance and power estimation, if any node tries to establish connection in our network, if this is in our range then our access controller provided true key for establish connection with some leniency otherwise if this is in outside the range then access controller provided fake random key for privacy. Several factors, including Path loss is the decrease in power density of a radio signal over a long distance. Path loss is more likely due to the gradual attenuation of radio signals over their extended journey.

The so-called inverse square law states that the radio wave power density increases as the square of the distance decreases. The sensitivity of the receiver is the second most essential factor in establishing a range. Fading margin and environmental circumstances are two other variables that must be accounted for in any computation. There is also a potential height effect on the measuring range, so be mindful of that while setting up your antenna. The accompanying graph depicts nonlinearity that is caused by the nonlinear effects of several different variables in the RF spectrum.

Future Scope

Biometric identifiers, fingerprints, voice samples, retina or iris information, and other forms of biometric identification all can be done for improvement in terms of security. A key's dependability may also be estimated using trust metrics built on top of the data records that make up blockchain. There will be a lot of testing of Io Chain's performance and sturdiness through the development of various apps on top of it. Also, the private Ethereum blockchain network has to be updated so that the PoS-based version of the ledger may be utilized, when it is published by Ethereum developers. To expand this work into healthcare, hospitality, pharmaceutical and education is possible in the future.

REFERENCES

[1] Achraf Fayad, Badis Hammi, Rida Khatoun "A Blockchain-based Lightweight Authentication Solution for IoT" Cyber Security in Networking Conference 2019.

[2] Aissam Outchkoucht, Hamza, Jean Philippe Leroy "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things" International Journal of Advanced Computer Science and Applications 2017.

[3] Soumyashree S. Panda, Utkalika Satapathy, Bhabendu K. Mohanta "A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices" IEEE 2019.

[4] Khadija Fazal1, Adeel M.Syed "Blockchain Authentication Mechanism for Securing Internet of Things" PakJET 2020.

[5] Dr. Sakthi Kumaresh, Dr. K B Priya Iyer "Decentralised Artificial Intelligence Enabled Blockchain Network Model" Turkish Journal of Computer and Mathematics Education 2021.

[6] Praveen Kumar Kollu, Monika Saxena, Khongdet Phasinam "Blockchain Techniques for Secure Storage of Data in Cloud Environment" Turkish Journal of Computer and Mathematics Education 2021.

[7] Shanshan Zhao, Shancang Li "Blockchain Enabled Industrial Internet of Things Technology" IEEE 2019.

[8] Muhammad Tahir, Muhammad Sardaraz , Shakoor Muhammad "A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics" Sustainability 2020.

[9] Dr Mohd Javaid, Prof. Abid Haleem, Dr Ravi Pratap Singh "Blockchain technology applications for Industry 4.0: A literaturebased review" Journal Pre-proof 2021.

[10] Bhabendu K. Mohanta, Anisha Sahoo, Shibasis Patel "DecAuth: Decentralized Authentication Scheme for IoT Device Using Ethereum Blockchain" IEEE 2019.

[11] Jesse Yli-Huumo, Deokyoon Ko, Sujin Cho "Where Is Current Research on Blockchain Technology? —A Systematic Review" PLOS ONE 2016.