Enhancing Security and Authentication System for Multi-WSN based Hybrid Blockchain and IoT Environment using ECDSA with Keccak Hashing Algorithms.

P. Velmurugadass [a]*, Dr. S. Dhanasekaran [b], Dr. V. Vasudevan [c]

[abc] Department of Computer Science and Engineering

[a-c] Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India - 626 126.

c

Abstract

With the speedy technological advancement and growth of sensors, WSNs have become the key technology for IoT. This inspires us to design our proposed system in a Multiwireless sensor network-based IoT environment. The main objective of our work is to provide a challenging standard of scalability, efficiency, and security in a multi-WSN system. With the intention of accomplishing our goal, we have implemented identity authentication based on hybrid blockchain technology. In this Distributed Multi WSN based IoT environment, the nodes are grouped into several ordinary nodes, cluster head nodes and base stations. In order to form a hybrid blockchain model, the blockchain network is created in among diverse types of nodes. On the one hand, the ordinary node's identity authentication is performed by the local blockchain. On the other hand, the cluster head's identity authentication is performed by a global blockchain. Thus, our intended private and public blockchain ensures extraordinary security and performance in the entire multi-WSN network. On the whole, our system proved that our proposed scheme has attained good security, scalability, and energy efficiency.

Keywords:

IoT, Blockchain, Multi-WSN, ECDSA Security and Hashing.

1. Introduction

In today's world, everything around us is connected with the environment. With the introduction of the Internet of Things (IoT) things started communicating with each other [8]. Cloud computing technology offers unlimited storage with other useful resources for people [19]. Researchers nowadays focus on working in the integrated domain environments, since the drawbacks of one domain are balanced by the advantages of the other domain. This showed a great increase in the realization of full potential of the number of domains being considered. Blockchain technology and Multi-WSN is one of the fast-spreading securities and decentralized approaches that replaced many existing security implementations [18].

Most of the time, these information are concerned about the experience of the user and the performance of the devices and system. The most common IoT devices are given in Fig. 1.

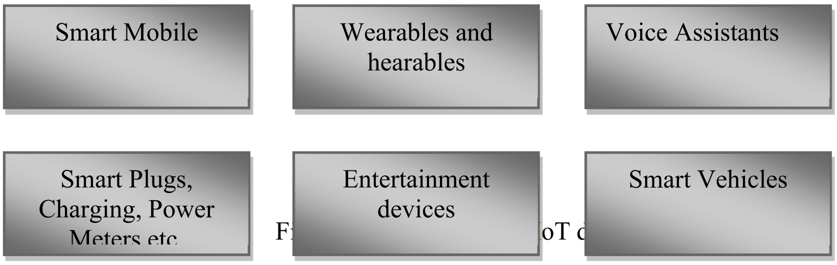


Figure1: Most Common IoT devices

nce issues associated with it. For this reason,

With all the benefits of IoT on one side, there are some bottlenecks such as poor scalability, security and performa the cloud computing technology created a breakthrough to solve these issues while promoting the wide spread growth of IoT. The importance of security has grown exponentially as the number of information present is vast and widespread. IoT shows a great impact in the interconnectivity of the environment where the disruptive technologies and solutions are developed [18].

Manuscript received November 5, 2024
Manuscript revised November 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.11.20

Applications of Internet of Things

- Smart everything with high efficiency.
- Growth of IoT in healthcare.
- Great improvement in the field of security.
- Develop huge data processing solutions.
- Improvement in automotive digital technology.
- A new buzz in industrial sector.
- Agriculture and Healthcare.

2. Literature Survey

[19] Zhang, X., Liu, C., Poslad, S., & Chai, K.K. (2019). Cloud computing has made a firm impact in the field of IoT devices such that IoT environment cannot be setup without the implementation of cloud. In general cloud services are obtained in three different forms as: Public, Private and Hybrid. Out of these most of the applications focus on private cloud as it offers high security compared with the public cloud. In this project, we implement our approach in untrusted cloud service (i.e.,) public cloud service. We develop and deployed a SemiOutsourcing Privacy Preserving (SOPP) scheme. In this project, the data from the IoT devices are first sent to the cloud for storage. The cloud verifies the identity of the IoT device and stores the data in the datacenter. The main objective of our proposed approach is to create a model that is suited for small-scale industries who cannot afford on storage from a trusted cloud. For the purpose of key generation we used, Elliptic Curve Diffie Hellman (ECDH) algorithm and Advanced Encryption Standard (AES) for the process of encrypting the IoT data. In order to verify the integrity of the data being stored in the cloud and to reduce the cost of communication, we have implemented One-way Hash function. With our proposed system, the data is stored securely in an untrusted cloud. The experimental results show that our proposed system is durable (i.e.,) supports long-term battery, and reduced throughput and thereby reducing the communication and computation overhead largely. Drawbacks

- Complexity in developing approach.
- Results are more inaccurate.

[20] Zhou, Y., Liu, T., Tang, F., & Tinashe, M. (2019). The research field of Internet of Things (IoT) exhibited many unique features than the other systems. With vast amount of applications and various characteristics, the IoT showed great performance in many areas. In this project, we have developed an unlinkable authentication scheme for distributed IoT applications. The main objective of the proposed system is to ensure an unforgeable authentication and to provide direct communication between the user and the sensors in the network. The three different entities present in our network are mobile users, sensors and trusted third party (TTP). The proposed system is 6 executed in three phases starting from the initialization phase, followed by the user registration phase and then the authentication phase. In each phase, the security is maintained in the hashed transfer of information and no information is leaked out of the system. Finally, the user can directly access the sensor for data transmission or data retrieval. Simulation results were conducted in terms of computation cost and running time which is greatly minimized in our proposed system. The experimental observation revealed that the proposed system exhibited better performance than the existing system.
Drawbacks

- Increased storage cost for handling resources.
- Not suited for real-time implementation.

[15] Renuka, K., Kumari, S., Zhao, D., & Li, L. (2019). The Internet of Things (IoT) area showed great improvement in recent years than the time of launch. Almost everything around us acts as IoT device and gathers useful information. IoT is deployed in all the fields around us. With the widespread application, it also suffers from certain security issues. In this project, we attempt to reduce the impacts of security issues in the IoT setup through the secure password based authentication scheme. We implemented four different protocols between the entities in the network and performed the authentication. For encryption and decryption, we deployed the symmetric encryption algorithm. As a result, the time and resources required for key generation and management is largely reduced. The four entities present in our system are: mobile devices, M2M service provider (MSP), sensors and gateway. In this paper we implemented four different protocols, each for separate authentication scenarios. The first protocol provides authentication between mobile devices and the gateway. The second protocol provides authentication between mobile devices and the sensor. The third protocol provides authentication between sensor and sensor with the gateway. The fourth protocol provides authentication between sensor and sensor without the gateway. The experimental analysis proved the hypothesis of the proposed system in term of reduced computation time and cost. Drawbacks

- Increased computation complexity.
- Not suited for resource constrained devices.

3. Methods

This research work applied different types of security methodologies with blockchain technology in the proposed framework structure.

4. Blockchain Technology

Blockchain technology is one of the fast-spreading security approaches that replaced many existing security implementations [13]. As the name indicates, this field consists of a chain of blocks containing certain information and more formally appears as a distributed ledger. It is a software protocol that could not be executed without the internet and comprises several components like a database, software application, and some connected computers. The information in each block is hashed and stored to enhance the level of security being offered.

It is observed that blockchain; hash algorithm function process is an excellent mechanism to prevent the security risks of data leakage. The specialty of a hash function is that even if the attacker enters into the block, they cannot get hold of the data as calculation of hashes is a tedious task. Also, blockchain makes use of the concept of Proof-of-Work [21]. It is a mechanism that slows down the creation of the new blocks. A proof-of-work is a computational problem that takes a certain effort to solve [17]. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself. Hybrid Blockchains lie somewhere between private and public blockchains, depending on their architecture [11]. Therefore, to understand hybrid blockchains, one must first understand the differences between private and public blockchains.

Advantages of Blockchain Technology

- Faster transactions.
- No payment for intermediaries Services.
- High level of security.
- Automatic reconciliation of accounts.
- Different levels of accessibility.
- Hacking threat reduced.
- Transparency of transactions increased.

5. Proposed Model

In this Figure 2 represent the developed hybrid blockchain based mutual authentication scheme for the Multi-WSN network. We initially divide the nodes in the multi-WSN network into normal nodes and cluster head nodes. Next we create the hybrid blockchain model which includes private and public blockchain. Then we authenticate the cluster members by local blockchain and authenticate cluster heads by global chain. For authentication, we have used ECDSA signature algorithm and Keccak hashing function. On the whole, this system ensures the scalability, security and efficiency. The performance evaluation shows that this approach has outperformed all the flaws in the existing system like,

- Unstable cluster head selection.
- Complex features are used for authentication.
- Improper authentication leads to malicious access of data.

The experimental analysis proved the hypothesis of the proposed system in terms of reduced computation time and cost. Authentication and security mechanism based on WSN, Access Point, Cluster Head, and End-user with the internet gateway.

Advantages of our proposed system

- Improved cluster head selection.
- Highly reliable and secure to implement.
- Increased efficiency and scalability.

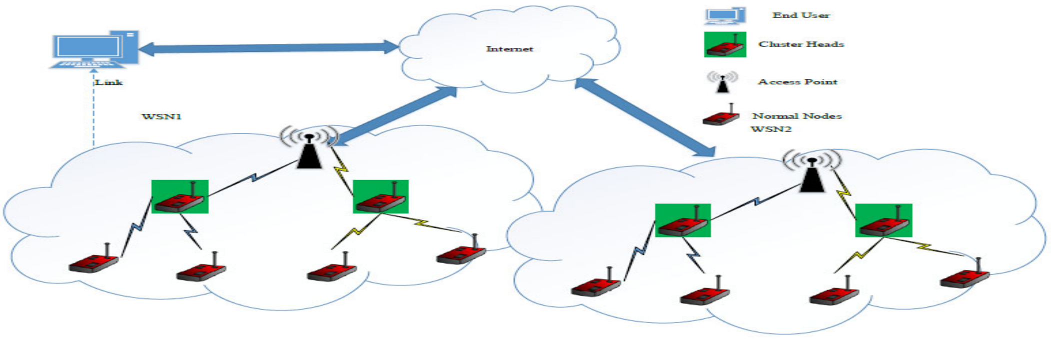


Figure 2: Propose Architecture system representation.

5.1 Module description

Initial Setup

We have considered a Multi- Wireless sensor network with the deployment of base station and several IoT devices or nodes. In the IoT environment, different sensor networks, networks and end users, and intra-network nodes need to cooperate to provide services. Then we initially calculate the important performance metrics in our system.

Clustering

According to the different functions and capability of the nodes, the nodes of the IoT are divided into base stations, cluster heads and ordinary nodes. The ordinary nodes act as cluster members. Cluster head node is mostly used for simple processing and forwarding sensing data from ordinary nodes in the network. It directly connects with the ordinary node and the base station, receives various data from the ordinary node and forwards it to the base station. Usually, ordinary nodes can only sense and transmit simple data because it has limited capacity and energy.

Local Blockchain

The local blockchain is a private blockchain composed of all cluster member nodes in a single WSN. Here it verifies the identity of all the ordinary nodes for communication. For that it implements the digital signature using ECDSA algorithm and hashing using keccak function.

5.2 Global Blockchain

The global blockchain is a public blockchain composed of all cluster head nodes in a single WSN. Here it verifies the identity of all the cluster head nodes for communication. For that, it implements the digital signature using the ECDSA algorithm and hashing using keccak function.

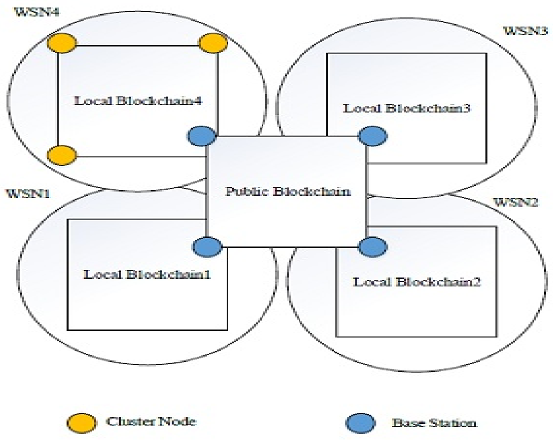


Figure 3 : Hybrid blockchain and Multi-WSN Network.

The above figure 3 represents the hybrid blockchain-based mutual authentication scheme for the Multi-WSN network. The Multi-WSN consists of 100 - IoT_Sensor Nodes and 1-Base Station (BS). We initially divide the nodes in the multi-WSN network into normal nodes and cluster head nodes. Next, we create the hybrid blockchain model which includes private and public blockchain. Then we authenticate the cluster members by local blockchain and authenticate cluster heads by a global chain. For authentication, we have used the ECDSA signature algorithm and Keccak hashing function. On the whole, this system ensures scalability, security, and efficiency. In finally, we plot the results graph for Accuracy vs a number of IoT Sensor Nodes and Authentication_Time vs a number of IoT Sensor Nodes. Hybrid blockchain and the Multi-WSN concept are used to improve attack detection and improve processing throughput [15]. This paper evaluated the performance of the Hybrid blockchain architecture evaluation results demonstrate performance improvement by reducing processing time, accuracy, and security parameters [7].

5.3 ECDSA algorithm

Digital Signature send by the sender to receiver is (r, s) and s can be generated only by Sender because of its private key.

Step 1: Compute s = (K + (r xnor h) G

Step 2: Compute s = (K + u) G where u = (r xnor h)

Step 3: Compute s = KG + uG

Step 4: Compute s - uG = KG = (k1, h1)

Therefore

LHS = KG = (k, g) and r = k (mod h)

RHS = SG = (k1, h1) and v = k1(mod h).

Hence v=r

ECDSA is one of the most efficient algorithms to protect from cyber attackers and this is used to generate a digital signature and verify the signature in a very fast manner. ECDSA is classified into key generation, signature generation with verification. ECDSA generates keys and signatures that are smaller to provide a security level and more efficient security. Simulation results were conducted in terms of computation cost and running time which is greatly minimized in our proposed system [20].

5.4 KECCAK Algorithm:

```
Step 1 : Start the process
for x= 0 to 100 do
begin
Step 2: Calculation of X and Y values
C[x][y]=a[x,0]
for y=1 to 100 do
begin
```

```
        $c[x]=c[x]\oplus a[x,y]$
      end if
    end if
Step 3: - Computation calculation
for x=0 to 100 do
begin
  $D[x] = C[x-1] \oplus ROT(C[x+1],1)$
Step 4: Bitwuse Rotatiion X and Y
  for y=0 to 100 do
  begin
    $A[x,y]=a[x,y]\oplus D[x]$
    $a[i][j][k] \leftarrow a[i][j][k] \oplus parity(a[0...100][j-1][k]) \oplus parity(a[0...100][j+1][k-1])$
    $0 \le t < 100, a[i][j][k] \leftarrow a[i][j][k-(t+1)(t+2)/2]$
    $x \leftarrow x \oplus (\neg y \& z)$
    $a[i][j][k] \leftarrow a[i][j][k] \oplus (\neg a[i][j+1][k] \& a[i][j+2][k])$.
  end if
end if
```

Keccak algorithm represents a hash function of the security of the IoT sensor node and the accuracy of message authentication. Numerical results show that the proposed architecture outperforms the traditional Multi-WSN architectures in terms of file security and network transmission. On average, the file loss rate based on the simulation assumptions utilized in this paper is close to 0% on the proposed architecture while it's nearly 100% and 71.66% on the architecture with a hybrid blockchain and the distributed proof of message using keccak algorithm [6]. Besides, with the proposed scheme, the transmission on the proposed architecture is reduced by 39.28% and 76.47% on average on the user's number and the number of file block replicas, respectively, in comparison to the architecture with the hybrid blockchain.

The random number To generation k with g(k1,h1). In the given key generation specified in equation (1) representing a digital signature verification and generation of the graph of hybrid blockchain structure. To protect user's privacy and to process private information security and authentication access [5].

$$G=(K1, H1) \tag{1}$$

Keccak hash function a unique feature and structure compare to other hash functions and K number of iteration in the function and every iteration has a sensor input of B1 bits values. In the function considered the number of iteration specified in equation (2) as

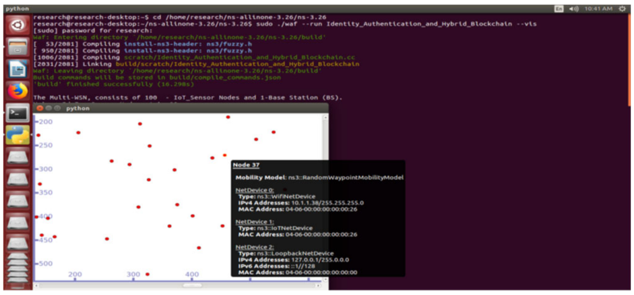
$$K= Node + Sensor + data + keyVal \tag{2}$$

Secure hash function to generate the secret key SecKey and verified that key in the equation (3) and (4).

$$SecKey = (PrivKey1Sender - PrivKey\ receiver\ ) \ / \ (hf1\text{-}fh2) \tag{3}$$

$$h = HASH\ (M) = Keccak\ (M) \tag{4}$$

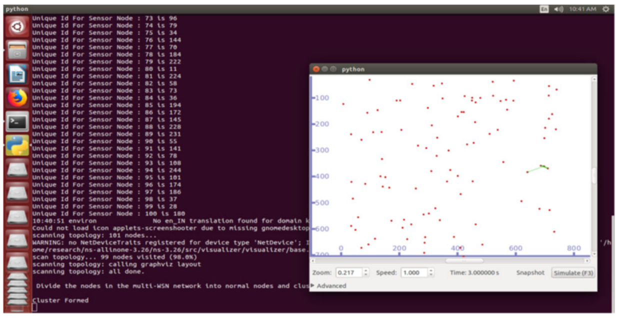
The ECDSA signature algorithm verifies an input message {r, s} produced from the digital signing algorithm plus a public key, matching to the signer's private key. The output process is based on boolean value: true or false signature. The digital signing algorithm consists of an equation for r and s messages. The ECDSA to solve the above problem by considering the private key generation and verification phas



```
research@research-desktop:~$ cd /home/research/ns-allinone-3.26/ns-3.26
research@research-desktop:~/ns-allinone-3.26/ns-3.26$ sudo ./waf --run Identity_Authentication_and_Hybrid_Blockchain --vis
[sudo] password for research:
Waf: Entering directory `/home/research/ns-allinone-3.26/ns-3.26/build'
[  53/2081] Compiling install-ns3-header: ns3/fuzzy.h
[ 950/2081] Compiling install-ns3-header: ns3/fuzzy.h
[1006/2081] Compiling scratch/Identity_Authentication_and_Hybrid_Blockchain.cc
[2031/2081] Linking build/scratch/Identity_Authentication_and_Hybrid_Blockchain
Waf: Leaving directory `/home/research/ns-allinone-3.26/ns-3.26/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (16.298s)

The Multi-WSN, consists of 100  - IoT_Sensor Nodes and 1-Base Station (BS).
```

```
Node 37

Mobility Model: ns3::RandomWaypointMobilityModel

NetDevice 0:
  Type: ns3::WifiNetDevice
  IPv4 Addresses: 10.1.1.38/255.255.255.0
  MAC Address: 04-06-00:00:00:00:00:26

NetDevice 1:
  Type: ns3::IoTNetDevice
  MAC Address: 04-06-00:00:00:00:00:26

NetDevice 2:
  Type: ns3::LoopbackNetDevice
  IPv4 Addresses: 127.0.0.1/255.0.0.0
  IPv6 Addresses: ::1//128
  MAC Address: 04-06-00:00:00:00:00:00
```

Figure 4 : M-WSN consists of 100 – IoT sensor Nodes

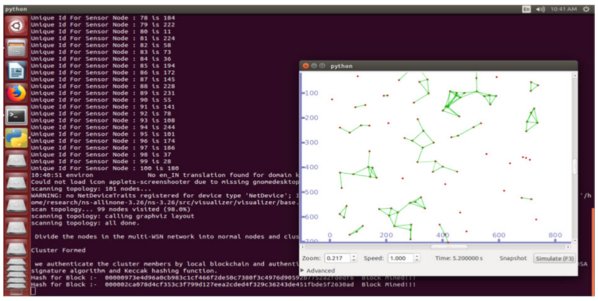


```
Unique Id For Sensor Node : 73 is 96
Unique Id For Sensor Node : 74 is 79
Unique Id For Sensor Node : 75 is 34
Unique Id For Sensor Node : 76 is 144
Unique Id For Sensor Node : 77 is 70
Unique Id For Sensor Node : 78 is 184
Unique Id For Sensor Node : 79 is 222
Unique Id For Sensor Node : 80 is 11
Unique Id For Sensor Node : 81 is 224
Unique Id For Sensor Node : 82 is 58
Unique Id For Sensor Node : 83 is 73
Unique Id For Sensor Node : 84 is 36
Unique Id For Sensor Node : 85 is 194
Unique Id For Sensor Node : 86 is 172
Unique Id For Sensor Node : 87 is 145
Unique Id For Sensor Node : 88 is 228
Unique Id For Sensor Node : 89 is 231
Unique Id For Sensor Node : 90 is 55
Unique Id For Sensor Node : 91 is 141
Unique Id For Sensor Node : 92 is 78
Unique Id For Sensor Node : 93 is 108
Unique Id For Sensor Node : 94 is 244
Unique Id For Sensor Node : 95 is 101
Unique Id For Sensor Node : 96 is 174
Unique Id For Sensor Node : 97 is 186
Unique Id For Sensor Node : 98 is 37
Unique Id For Sensor Node : 99 is 28
Unique Id For Sensor Node : 100 is 180
10:40:51 environ              No en_IN translation found for domain k
Could not load icon applets-screenshooter due to missing gnomedesktop
scanning topology: 101 nodes...
WARNING: no NetDeviceTraits registered for device type 'NetDevice'; I
ome/research/ns-allinone-3.26/ns-3.26/src/visualizer/visualizer/base.
scan topology... 99 nodes visited (98.0%)
scanning topology: calling graphviz layout
scanning topology: all done.

 Divide the nodes in the multi-WSN network into normal nodes and clus

Cluster Formed
```

Zoom: 0.217 Speed: 1.000 Time: 3.000000 s

Figure 5: M-WSN Network and Cluster head nodes

In the above figure 4 and 5 represent the IoT devices message delivery system with multi-WSN processing then initially divide the nodes in the multi-WSN network into normal nodes and cluster head nodes. The Multi-WSN, consists of 100 – IoT Sensor Nodes and 1-Base Station (BS) and output process generated based on base station input node message processing.



```
Unique Id For Sensor Node : 78 is 184
Unique Id For Sensor Node : 79 is 222
Unique Id For Sensor Node : 80 is 11
Unique Id For Sensor Node : 81 is 224
Unique Id For Sensor Node : 82 is 58
Unique Id For Sensor Node : 83 is 73
Unique Id For Sensor Node : 84 is 36
Unique Id For Sensor Node : 85 is 194
Unique Id For Sensor Node : 86 is 172
Unique Id For Sensor Node : 87 is 145
Unique Id For Sensor Node : 88 is 228
Unique Id For Sensor Node : 89 is 231
Unique Id For Sensor Node : 90 is 55
Unique Id For Sensor Node : 91 is 141
Unique Id For Sensor Node : 92 is 78
Unique Id For Sensor Node : 93 is 108
Unique Id For Sensor Node : 94 is 244
Unique Id For Sensor Node : 95 is 101
Unique Id For Sensor Node : 96 is 174
Unique Id For Sensor Node : 97 is 186
Unique Id For Sensor Node : 98 is 37
Unique Id For Sensor Node : 99 is 28
Unique Id For Sensor Node : 100 is 180
10:40:51 environ              No en_IN translation found for domain k
Could not load icon applets-screenshooter due to missing gnomedesktop
scanning topology: 101 nodes...
WARNING: no NetDeviceTraits registered for device type 'NetDevice'; I                    '/h
ome/research/ns-allinone-3.26/ns-3.26/src/visualizer/visualizer/base.
scan topology... 99 nodes visited (98.0%)
scanning topology: calling graphviz layout
scanning topology: all done.

 Divide the nodes in the multi-WSN network into normal nodes and clus

Cluster Formed

 we authenticate the cluster members by local blockchain and authenti                    SA
signature algorithm and Keccak hashing function.
Hash for Block :-  00000973e4d96a0cb983c1cf466f2de50c7380f3c4976d90592b77752a2fdedf6  Block Mined!!!
Hash for Block :-  000002ca078d4cf353c3f799d127eea2cded4f329c36243de451fbde5f2630ad  Block Mined!!!
```

Figure 6: Hybrid Blockchain

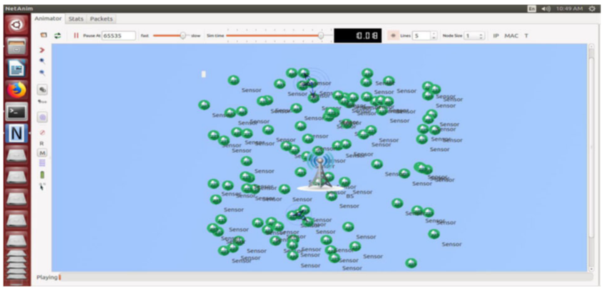


Figure 7 : Simulation of IoT Sensore

In this figure 6 represent a hybrid blockchain model which includes private and public blockchain. Then we authenticate the cluster members by local blockchain and authenticate cluster heads by global chain. For authentication, we have used ECDSA signature algorithm and Keccak hashing function.

A figure 7 represent the Simulation of IoT Sensors results demonstrated that the proposed system successfully completed based IoT Sensor node message, Multi-Wireless sensor network with the deployment of the base station using Hybrid blockchain Proof of Stake (PoS) then reduce power to run different types of IoT device messages authentication verified based on algorithms. This simulation result used to verify the IoT notes message authentication to assess the practicality of secure provenance schemes. However, the communication of Multi-wireless network overhead will increase dramatically when users transmit files encrypted by an authentication verification based on the PoS scheme. A numerical result shows that simulation of IoT sensors and outperforms the traditional Multi-Wireless and Hybrid blockchain architectures in terms of file security and network transmission delay.

6. The results graph for Accuracy vs number of IoT Sensor Nodes

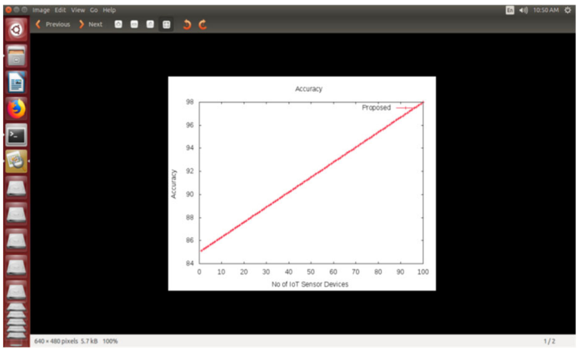


Figure 8 : Accuracy vs number of IoT Sensor Nodes

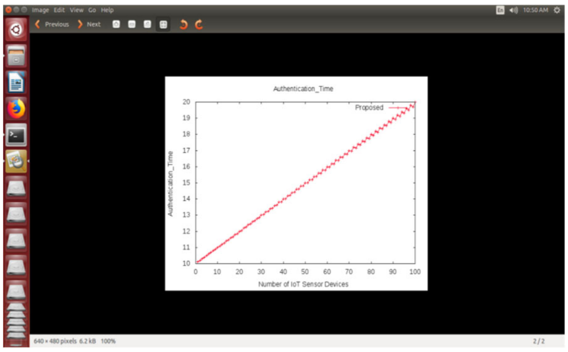


Figure 9 Authentication time vs number of IoT Sensor Node

In the above figure 8 represent IoT devices and blockchain based message authentication and accuracy of data protection such as the sensor node generate the message that time accuracy also calculated based on number of sensor devices are connected to Multi-WSN . X axis denoted here 100 number of sensor devices, Y- axis denote accuracy of message delivery and time complexity. Finally in this output had generated 100 % accuracy message with message authentication and time complexity.

Figure 9 represent the authentication of message verification time and number of sensor node producing result based an input message with IoT nodes. In equation (5) is verified a Sensor Node message and calculate a result based an activity score and an average of the time (T) with sensor node (N) scores weight and results calculated based on output 98% and based on input message of IoT devices and OSC- Output Score Calculation.

$$OSC= SN+ \gamma A+(1-\gamma)SI=\gamma A+(1-\gamma)S \qquad (5)$$

$$MM = 1 + 3b + 3b^2 + (3b)(3b+1) + 3b+1 \qquad (6)$$

In this equitation (6) denoted MM is a number of message modifications, γγ - Network activity factor indication, 1 is a base node of the network and 'b' denoted block of message proof of transaction. ECDSA with Keccak to secure authentication for IoT device messages to ensure and enhance the security of the system. In this output result, we propose a lightweight and privacy-preserving two-factor authentication scheme for IoT devices with blockchain technology. Our research is developed with the intention of providing reduced computation such that it is suitable for a resource-constrained environment. The experimental analysis confirmed that our proposed approach is suitable for the application or environment with resource-constrained devices and a lightweight authentication mechanism reduces the overhead largely.

7. Conclusion

In this research, we have proposed a Multi-WSN network in an IoT environment. We deployed hybrid blockchain technology to assure the security of data in a distributed environment. We considered the most significant parameters that most of the existing systems failed to consider in their implementations. These parameters include scalability, storage consumption, energy consumption which ensures the efficiency of the proposed system. This hybrid blockchain model has a private blockchain and public blockchain. The private blockchain is built among cluster heads in a single WSN and base stations of all WSN are added to the public blockchain. In this model, nodes identity mutual authentication in various communication scenarios is recognized. The local blockchain authenticates the ordinary nodes and the global blockchain authenticates the cluster heads. Thus, our system achieved increased efficiency, security, and scalability than the existing system.

8. Future work

In the future, we have planned to implement multi-factor authentication to enhance the security of the proposed system. We also keep in mind that the computation complexity is controlled and that our system is suitable for resource-constrained IoT devices. We will also make our system to be suited for more complicated and large-scale environments.

References

[1] Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark. IEEE Transactions on Network and Service Management, 16, 936-949.

[2] Abdullaziz, O.I., Wang, L., & Chen, Y. (2019). HiAuth: Hidden Authentication for Protecting Software Defined Networks. IEEE Transactions on Network and Service Management, 16, 618-631.

[3] Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E., & Djaba, E. (2019). Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT Using One-Time Pads. IEEE Internet of Things Journal, 6, 3925-3933.

[4] Cai, X., Zhang, J., Liang, H., Wang, L., & Wu, Q. (2019). An ensemble bat algorithm for large-scale optimization. Int. J. Mach. Learn. Cybern., 10, 3099-3113.

[5] Cai, X., Niu, Y., Geng, S., Zhang, J., Cui, Z., Li, J., & Chen, J. (2020). An under-sampled software defect prediction method based on hybrid multi-objective cuckoo search. Concurrency and Computation: Practice and Experience, 32.

[6] DONG ZHENG1,2, AXIN WU1 , YINGHUI ZHANG1,2, AND QINGLAN ZHAO (2018) Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power. IEEE Access DOI: 10.1016/j.ins.2018.06.071.

[7] Gope, P., & Hwang, T. (2016). A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. IEEE Transactions on Industrial Electronics, 63, 7124-7132.

[8] Gope, P., & Sikdar, B. (2019). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. IEEE Internet of Things Journal, 6, 580-589.

[9] Khan, Z., Fan, P., Abbas, F., Chen, H., & Fang, S. (2019). Two-Level Cluster Based Routing Scheme for 5G V2X Communication. IEEE Access, 7, 16194-16205.

[10] Kumar, D., Chand, S., & Kumar, B. (2019). Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Journal of Ambient Intelligence and Humanized Computing, 10, 641-660.

[11] Kersic, V., Stukelj, P., Kamisalic, A., Karakatič, S., & Turkanovic, M. (2019). A Blockchain- and AI-based Platform for Global Employability. BLOCKCHAIN.

[12] Liu, J., Tang, H., Sun, R., Du, X., & Guizani, M. (2019). Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud. IEEE Access, 7, 106951-106961.

[13] Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., & Zhang, Z. (2018). CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. IEEE Transactions on Intelligent Transportation Systems, 19, 2204-2220.

[14] Liu, M., Yu, F., Teng, Y., Leung, V.C., & Song, M. (2019). Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing. IEEE Transactions on Wireless Communications, 18, 695-708.

[15] Renuka, K., Kumari, S., Zhao, D., & Li, L. (2019). Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems. IEEE Access, 7, 51014-51027.

[16] Sharaf, S., & Shilbayeh, N. (2019). A Secure G-Cloud-Based Framework for Government Healthcare Services. IEEE Access, 7, 37876-37882.

[17] Shae, Z., & Tsai, J. (2019). AI Blockchain Platform for Trusting News. 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 1610-1619.

[18] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand ,V. Vasudevan. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm, Materials today proceeding Volume 37, Part 2, 2021, Pages 2653-2659.

[19] Zhang, X., Liu, C., Poslad, S., & Chai, K.K. (2019). A Provable Semi-Outsourcing Privacy Preserving Scheme for Data Transmission From IoT Devices. IEEE Access, 7, 87169-87177.

[20] Zhou, Y., Liu, T., Tang, F., & Tinashe, M. (2019). An Unlinkable Authentication Scheme for Distributed IoT Application. IEEE Access, 7, 14757-14766.

[21] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019). A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. IEEE Internet of Things Journal, 6, 8114-8154.

Mr P.Velmurugadass B.Sc.,MCA.,B.Ed.,M.Tech.,(P.hD)., is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India, he received his B.Sc in Computer Science from Madurai Kamaraj University, Madurai, Tamil Nadu, India in the year of 2003, MCA in Computer Applications from Madurai Kamaraj University, Madurai, Tamil Nadu, India in the year of 2007, B.Ed in Computer Science from Tamil Nadu Teachers Education University, Chennai, Tamil Nadu, India in the year of 2015, M.Tech in Information technology from Sathyabama University, Chennai, Tamil Nadu, India in year of 2013 and P.hD pursuing in Computer Sciencecs and Engineering from Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India. He has 13 years of experience in teaching. He has published books of Professional Ethics. he has delivered guest lecturers in IDE University of Madras.

Dr. S.Dhanasekaran is currently working as an Associate Professor in the Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India, he did SSLC & HSC in the year 1998 & 2000 respectively from Mangapuram Hindu Nadar Higher Secondary School, Srivilliputtur. He had finished his Under Graduate Degree, B.E., in Computer Science and Engineering from Madurai Kamarajar University, Tamilnadu, with first class in the year 2004. He has received Post Graduate Degree M.E., (CSE) in First class with Distinction from Annamalai University, Tamilnadu in the year 2007. He has started his Academic career as Lecturer in Department of IT in Arulmigu Kalasalingam College of Engineering (AKCE) in 2008.He has completed Ph.D., (Cloud Computing) in the year 2017 at Kalasalingam University

Sr. Prof Dr V.Vasudevan - Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India. Registrar He has a maths PhD, headed MCA dept of Kalasalingam University from 1997 to 2003 .Then headed the IT dept for over ten years. During the same period i was the chief suprindetent of university exams for 6 years, Dean hostels for four years, Dean admissions & dean placements for three years from 2011 to 2014 .then currently working as a Registrar from 2013.so for 25 students completed Phd under my guidance and he has the credit 67 international publications . He has 25 years of experience in teaching and research experience.