BLOCKCHAIN BASED SMART TRAFFIC SYSTEM TO ENHANCE TRAFFIC NEUTRALITY

Mrs.P.Sheela Rani M.E.[1], K.Lavanya[2], B.Tharani[3], R.R.Ramya Fathima

[1]*Associate Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai.*
[2,3,4]*UG Scholar Department of Information Technology, Panimalar Institute of Technology, Chennai.*

---***---

Abstract - *Security and privacy of a traffic system is extremely crucial since it involves social flow and even lives, and thus we have the need to develop a new system that is more secure and private and can overcome many difficulties faced by common existing systems. We implement the concept of blockchain to overcome those security difficulties. Since blockchain always incorporate decentralized systems, there are very few chances to hack into the systems or infect any malicious attacks into it. We propose a decentralized system to address the data integrity along with the privacy-preserving issues in blockchain-based traffic management systems.Our proposed architecture integrates with permissioned and modular blockchain network called Hyperledger Fabric which establish decentralized trust in a network of known participants rather than an open network of anonymous participants. It exposes only the data you want to share to the parties you want to share it with thus enhancing the traffic neutrality of the data.We also use Attribute Based Encryption along with Identity Based Encryption called Encryption Security protocol(EPS), therefore doubling upon security of the traffic system.By using this both algorithms , we are making sure that Man in the Middle attack , Denial of Service attacks are prevented using this standard encryption techniques.Through this system, we can be able to achieve a secure and smart traffic management system which provides more security and privacy to user's data.*

Key Words: Blockchain, Hyperledger fabric, Attribute Based Encryption, Identity Based Encryption, Security Privacy, Data neutrality

I. INTRODUCTION

Emerging adaptive traffic signal control systems incorporate real- time traffic data in their signal phase and timing (SPaT) mechanisms to improve the performance of intersections (e.g., safety and throughput). However, centralized traffic signal control systems and their data centers can be attacked by receiving and processing malicious messages from connected vehicles in the traffic network. These malicious messages can include false information about vehicle IDs, locations, trajectories, etc. Systematic malicious attacks are a major challenge for traffic data centers that need to validate a large amount of vehicular data for making decisions in real time. Without a trustable defending mechanism, malicious information could lead to serious consequences in a traffic network such as collisions and congestions. In this paper, we present a blockchain-based architecture to defend intelligent traffic signal control systems against information and data attacks by transforming the conventional connected vehicle network into a trustable and transparent decentralized network.As an emerging computer network technology, blockchain was first invented in a cryptocurrency system, Bitcoin . In the past few years, blockchain- based system designs have come a long way, and they have been successful in various decentralized applications .The nature of traceability and transparency in blockchain has a suitable match with increasing demands for data security in the connected-vehicle networks. However, most blockchain-based applications depend largely on digital tokens for the system design. This limits blockchain technology to be implemented mostly in cryptocurrency related systems . In this paper, we extend blockchain technology from classic cryptocurrency systems into traffic signal control systems. Blockchain not only links vehicles and infrastructures together in a decentralized network but also it works as a distributed and immutable ledger to automatically record vehicular information with timestamps. Furthermore, this distributed ledger provides trustable input data directly for intelligent traffic signal control systems.

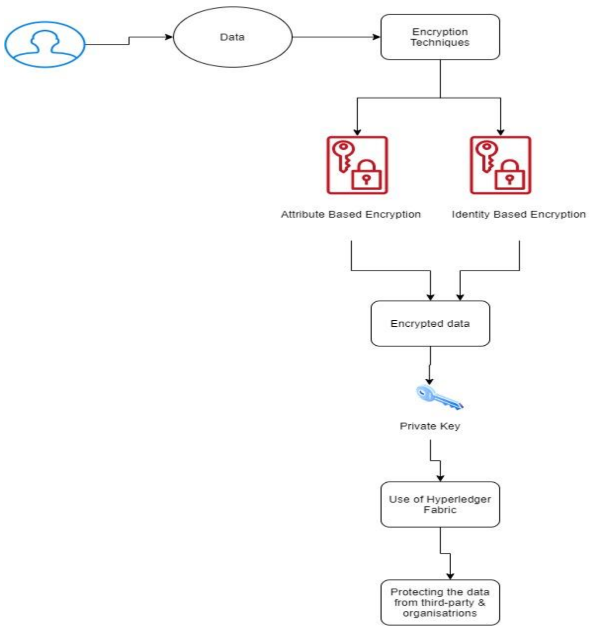
II. PROBLEM DEFINITION

The privacy of the user's data is less as sensitive data is integrated on a public blockchain. Permissionless blockchain based traffic systems are vulnerable to hacks and malicious attacks. As a result, the traffic system can not only deliberately return malicious route plans to users, but also track users and cause serious security concerns.

III. PROPOSED APPROACH

We propose a decentralized system to address the data integrity along with the privacy-preserving issues in blockchain-based traffic management systems. Our proposed architecture integrates with permissioned and modular blockchain network called Hyperledger Fabric which establish decentralized trust in a network of known participants rather than an open network of anonymous participants. It exposes only the data you want to share to the parties you want to share it with thus enhancing the traffic neutrality of the data. It also uses Attribute Based Encryption along with Identity Based Encryption called Encryption Security protocol(EPS), therefore doubling upon security of the traffic system. By using this both algorithms , we are making sure that Man in the Middle attack , Denial of Service attacks are prevented using this standard encryption techniques.

IV. ARCHITECTRE DIAGRAM


Data
Encryption Techniques
Attribute Based Encryption
Identity Based Encryption
Encrypted data
Private Key
Use of Hyperledger Fabric
Protecting the data from third-party & organisatrions

V. MODULES IN THE SYSTEM

??. Encrypting traffic data
??. Storing the data as blocks
??. Security using Hyperledger fabric

1. Encrypting user data

Traffic data contains important information about vehicle No, Vehicle insurance and many more various data. These data should be highly secured since many organizations have been trying to use this data for various illegal purposes. So we are going to encrypt this data by using two standard encryption algorithms

Attribute Based Encryption

In Attribute based encryption, the data is encrypted based on several attributes, Say for example, in the encryption of vehicle data, here the attributes are vehicle no and vehicle id. These are the 2 attributes of the encryption. Based on this 2 attributes the encryption is done. Now for the decryption part, anyone who has the vehicle no attribute and vehicle id attribute can decrypt the data. If a person has either one of the attribute, he can't decrypt the data. This is the major advantage of the attribute based encryption. The attributes are considered as the key and this attributes can be from 1 to many depending upon the encryption.

Identity Based Encryption

In Identity based encryption , the data is encrypted based on several identities , Say for example , in the encryption of data , considering the data is "john , this vehicle has no insurance", here the identity is "john" Based on this identity the encryption is done . Now for the decryption part, anyone who has knows this identity can decrypt the data.

2. Storing the data as blocks

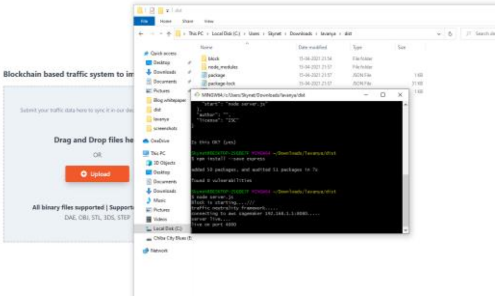
In this module, the data are stored as blocks to ensure more security, the blocks are created in a order so that every new block contains the hash value of the previous block. Every block is hashed before it is being stored. The encrypted data is stored in blocks and even if any hackers or any organizations tries to access the data, the data is well encrypted using standard encryption techniques and only authenticated person can access the data

3. Security using Hyperledger fabric

This is the module where the data stored is made secure using Hyperledger fabric .Hyperledger is an open-source, distributed blockchain project—Suitable chain technology for the enterprise. Hyperledger Fabric is an implementation of the blockchain architecture and one of the Hyperledger projects hosted by The Linux Foundation. It uses container technologies to provide modular architecture and pluggable, interchangeable facilities. To enable permissioned networks, Hyperledger Fabric provides a membership identity service that manages user IDs and authenticates all participants on the network. Access control lists can be used to provide additional layers of permission through authorization of specific network operations.

VI.EXPERIMENTS AND RESULTS

MODULE 1:



Blockchain based traffic system to im

Submit your traffic data here to sync it in our de

Drag and Drop files he

OR

All binary files supported | Support

DAE, OBJ, STL, 3DS, STEP

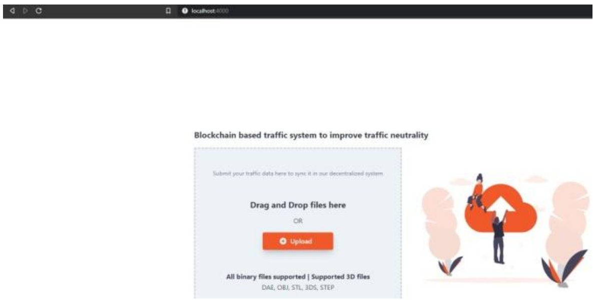
This PC › Local Disk (C:) › Users › Skynet › Downloads › lavanya › dist

Name	Date modified	Type	Size
block	15-04-2021 21:54	File folder	
node_modules	15-04-2021 21:57	File folder	
package	15-04-2021 21:57	JSON File	1 KB
package-lock	15-04-2021 21:57	JSON File	31 KB

MINGW64:/c/Users/Skynet/Downloads/lavanya/dist

```
  "start": "node server.js"
 },
 "author": "",
 "license": "ISC"
}


Is this OK? (yes)

Skynet@DESKTOP-[illegible] MINGW64 ~/Downloads/lavanya/dist
$ npm install --save express

added 50 packages, and audited 51 packages in 7s

found 0 vulnerabilities

Skynet@DESKTOP-[illegible] MINGW64 ~/Downloads/lavanya/dist
$ node server.js
Block is starting....///
traffic neutrality framework.....
connecting to aws sagemaker 192.168.1.1:8080.....
server live....
live on port 4000
```

MODULE 2:



localhost:4000

Blockchain based traffic system to improve traffic neutrality

Submit your traffic data here to sync it in our decentralized system

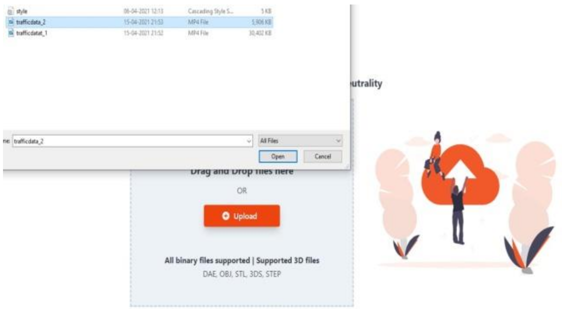
Drag and Drop files here

OR

All binary files supported | Supported 3D files

DAE, OBJ, STL, 3DS, STEP

MODULE 3:



style	08-04-2021 12:13	Cascading Style S...	1 KB
trafficdata_2	15-04-2021 21:53	MP4 File	5,906 KB
trafficdata_1	15-04-2021 21:52	MP4 File	30,402 KB

File name: trafficdata_2

All Files

utrality

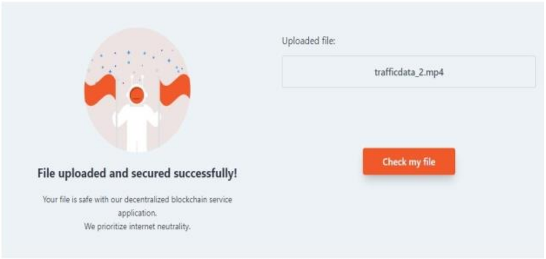
Drag and Drop files here

OR

All binary files supported | Supported 3D files

DAE, OBJ, STL, 3DS, STEP

MODULE 4:



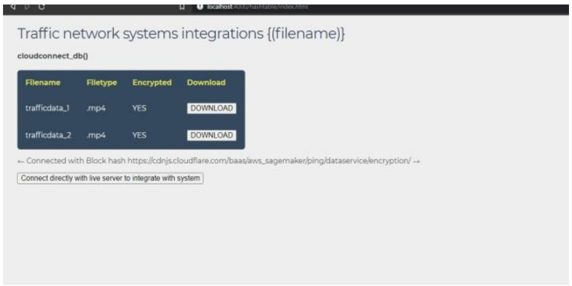
File uploaded and secured successfully!

Your file is safe with our decentralized blockchain service application.
We prioritize internet neutrality.

Uploaded file:

trafficdata_2.mp4

MODULE 5:



localhost:4000/hashtable/index.html

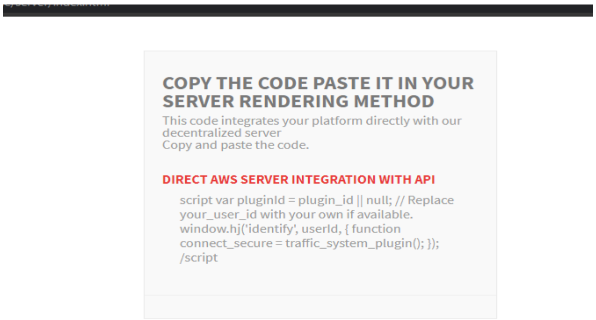
Traffic network systems integrations {(filename)}

cloudconnect_db()

Filename	Filetype	Encrypted	Download
trafficdata_1	.mp4	YES	DOWNLOAD
trafficdata_2	.mp4	YES	DOWNLOAD

← Connected with Block hash https://cdnjs.cloudflare.com/baas/aws_sagemaker/ping/dataservice/encryption/ →

MODULE 6:



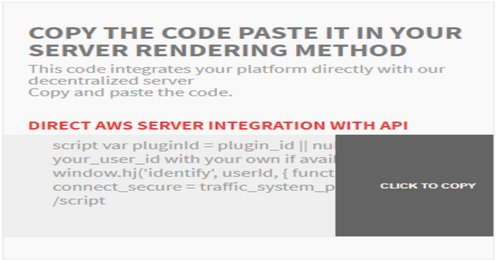
COPY THE CODE PASTE IT IN YOUR SERVER RENDERING METHOD

This code integrates your platform directly with our decentralized server
Copy and paste the code.

DIRECT AWS SERVER INTEGRATION WITH API

```
script var pluginId = plugin_id || null; // Replace
your_user_id with your own if available.
window.hj('identify', userId, { function
connect_secure = traffic_system_plugin(); });
/script
```

MODULE 7:



COPY THE CODE PASTE IT IN YOUR SERVER RENDERING METHOD

This code integrates your platform directly with our decentralized server
Copy and paste the code.

DIRECT AWS SERVER INTEGRATION WITH API

```
script var pluginId = plugin_id || nu
your_user_id with your own if avai
window.hj('identify', userId, { funct
connect_secure = traffic_system_p
/script
```

VII .CONCLUSION

Thus using block chain and hyper ledger fabric an effective security system was implemented . Also now a days security is one of the big concern in the internet and many people are afraid of leakage of the private data to other organizations. Our Proposed system ensures that all the data of the users are safely secured ensuring maximum privacy of the data . We will be storing all data into blocks and every block will be created after the first block contains the hash of the previous block's data. In this way the man in the middle attack and data leakage will be prevented.

FUTURE SCOPE

The future scope includes deploying this system as web application in any cloud platforms . Also the performance of the system can be improved . More security mechanisms and additional encryption techniques can be added to improve the security

REFERENCES

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in Proc. 2nd Int. Conf. Internet-Things Design Implement.
(IoTDI), 2017, pp. 173–178.

[2] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[3] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "SpeedyChain: A framework for decoupling data from blockchain for smart cities," in Proc. 15th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services, 2018, pp. 145–154.

[4] L.-A. Hirtan and C. Dobre, "Blockchain privacy-preservation in intelligent transportation systems," in Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE), Oct. 2018, pp. 177–184.

[5] S. E. Jabari and H. X. Liu, "A stochastic model of traffic flow: Gaussian approximation and estimation," Transp. Res. B, Methodol., vol. 47, pp. 15–41, Jan. 2013.

[6] C. Wang, X. Li, X. Zhou, A. Wang, and N. Nedjah, "Soft computing in big data intelligent transportation systems," Appl. Soft Comput., vol. 38, pp. 1099–1108, Jan. 2016.

[7] H. Zhu, X. He, X. Liu, and H. Li, "PTFA: A secure and privacy-preserving traffic flow analysis scheme for intelligent transportation system," Int. J. Embedded Syst., vol. 8, no. 1, pp. 78–86, 2016.

[8] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2703–2713, Mar. 2017.

[9] Y. Zhang, Q. Pei, F. Dai, and L. Zhang, "Efficient secure and privacy preserving route reporting scheme for VANETs," J. Phys., Conf. Ser., vol. 910, nol. 1, Oct. 2017, Art. no. 012070.

[10] R. Rajbhandari, "Exploring blockchain-technology behind bitcoin and implications for transforming transportation," Texas A&M Transp. Inst., College Station, TX, USA, Tech. Rep., 2018.

[11] P. G. Saranti, D. Chondrogianni, and S. Karatzas, "Autonomous vehicles and blockchain technology are shaping the future of transportation," in Proc. 4th Conf. Sustain. Urban Mobility. Cham, Switzerland: Springer, 2018, pp. 797–803.

[12] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2016, pp. 2663–2668.

[13] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in Proc. Int. Smart Cities Conf. (ISC), Sep. 2017, pp. 1–4.

[14] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," 2017