**Blockchain Based Zero Knowledge Proof Model for Secure Data Sharing Scheme in a Distributed Vehicular Networks**

Muhammad Umar Majigi1, Ismaila Idris2, Shafii M. Abdulhamid3, Richard Adeyemi Ikuesan4

Andrew Anogie Uduimoh5,

1, 2, 3,5 Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.

4 Department of Cybersecurity and Networking. Community College of Qatar Doha, Qatar

1majigiumar1@gmail.com, 2ismi.idris@futminna.edu.ng

**ABSTRACT**

The possibility of implementing advanced applications, such as improved driving safety, has increased with the rapid development of vehicular telematics, and existing vehicular services have been enriched through data sharing and analysis between vehicles. This research uses smart contracts and consortium blockchain zero knowledge proof to secure data sharing and storage in vehicular networks. The results indicate that, for message sizes (m), both data\_ experiments \_2 and 1 produce ciphertext of the same size, with the exception of 'gnfuv-temp-exp1-55d487b85b-5g2xh,' which generates ciphertext of 156 bits with the lowest decryption time of 26,865ms and a small decrease in encryption time between 28,620ms and 28,162ms. the proposed model validation shows that the model performed better than Advanced encryption standard in term of ciphertext size, encryption time and decryption time in comparison and it satisfies the good and robust blockchain-based zero knowledge proof model for secure data sharing and storage for distributed VANET. The scheme achieves high levels of security while operating with reasonable efficiency, reliability and availability according to numerical results.

**Keywords**: Blockchain, Vehicular Networks, Zero Knowledge Proof, Certificate authority, Roadside units, Data sharing

**1. Introduction**

With the rapid development of vehicular applications and telematics, huge amount of data will be required by the vehicles to share information. For instance, a vehicle on motion/self-driving can create 1gigabyte of data per second from GPS, radar and cameras [1]. Furthermore, data of common interest are share and collected by vehicles [2], [3]. Collected data by the vehicles consists of subjective and objective information. Traffic related data, for example road and weather conditions and parking lot occupancy are known as Objective information. The quality of vehicular services and rating of hotel are subjective information [4]. With data sharing it is possible to realize certain goals such as obtaining service quality during travelling and enhanced driving safety.

Large scale data sharing and enormous data storage in vehicles are not sustainable due to resource constraints. Data transmission increasingly becomes complex due to large data generated by vehicles. Traffic information are locally relevant data for vehicles with spatial scope and overt lifetime of utility which requires location awareness and low latency for vehicular data sharing [2]. In order to address the above challenges, Mobile edge computing is required which is a promising paradigm that can be implanted at the network edge infrastructures, for example Road-side Units (RSUs), to support immense data storage, sharing and computing near to the vehicles [2], [5]. Privacy and security problems are perilous challenges for vehicular network (VANET) due to risk of single point of failure (SPoF) and data leakage in the centralized server slant. It is therefore essential for further studies on designing a secure data management system in VANET without an intermediary [6][7].

The data sharing in a VANET contain critical data of users which make data privacy increasable significant in the areas of data storage [7]. Consequently, the register members are unenthusiastic due to risk of different malicious activities in sharing and storing of their data in the system that will endanger security of the system and members privacy. Preferably, as the data management still remains untrusted all data are sent all data are incognito to overcome the problem. It is important to note that real Identity of a user cannot be reveal. However, data reliability is not assured but it can solve privacy violation risk. Furthermore, the user’s share data and make it possible to assessing data integrity for other user as reduced due to lack of reward [8]. Thus, the incentives mechanism nature is leveraged on to encourage vehicles and user to share and store their data while evaluating the trustworthiness of data in VANET.

Since Nakamoto introduced Bitcoin [9], in the past ten years blockchain has gained much popularity as an emerging technology to provide better security on data sharing among many parties without an intermediary. Blockchain is known as an suitable solution that address the privacy security issue [10], in the last years when Nakamoto introduced Bitcoin [9], [11] blockchain has gained much popularity as an emerging technology in providing better security on data sharing without intermediary, which can simplify a trusted, secure, trusted and decentralized smart transportation system.

In 2008 Satoshi Nakamoto introduces blockchain technology [16] to provide best security, establish trust entities and ensure privacy. With the increasing number of records stored in the form of blocks, when joined together in a chronological order to form a chain using cryptographic hashes. Multiple components are found in a block, for instance a cryptographic hash of the prior block, timestamp in which block is generated, transaction data are in the form of Merkle root tree and nonce, which is arbitrary number used for mining process.

The research has established the following contributions:

1. The research has established a stronger symmetric key generation approach for VANET data sharing and storage.
2. Proposes consortium blockchain and zero knowledge proof to establish a secure and distributed vehicular blockchain for data management in VANET.
3. Deploying zero knowledge proof on the vehicular blockchain for secure vehicles data sharing and efficient data storage on RSUs.

**2. Related Work**

In trustless infrastructures, Blockchain technology is the most powerful tool that address data management issues. Blockchain layer controlled all the operations handled on data and also easy to detect all abuse on the data. In this research, literatures proposed several blockchain that addresses storage and data sharing problems.

A decentralized solution was proposed by [12] for effective data sharing in IoT environment with a distributed data storage system. The proposed system uses blockchain to maintain data access control and data storage model. This later is ensured using blockchains in decentralized manner. However, the proposed solution did not consider the privacy issues that are very important to address in the context of IoT applications. Also, [13] proposed a data sharing blockchain-based architecture for healthcare that will manage three layers to access to private ERH (Electronic Medical Record) related to patient’s cases. The different users will occupy first layer that are potentially interested to access the patients’ data. The blockchain used as a storage data layer is manage based on the access control. Besides the invariability property of blockchain, the ERH are encrypted and inked to ensure the confidentiality, integrity and authenticity of data.

[14] built identity management system which depend on third party called identity verifier to authenticate the user with the privacy, that acts as the trusted party for user to be able prove his identity to the service enabler, the identity verifier and partial information proves it correctness. When using the interactive ZKP mode, six miners must confirm the transaction before it can be considered accepted and recorded on the ledger. [15] interactive implementation is yet another tool for creating secure auction systems and only needs four confirmations from miners. There is no direct communication between the parties, and the private data is kept on a central ledger that is overseen by a reliable third party.

To verify the accuracy of the model prediction process without disclosing the private parameters or key of the deep learning model, [18] propose a deep learning integrity verification scheme. In order to prove the viability and applicability of the plan, the proving party completes the proof circuit design for each layer of the model using the ZKP system zk-SNARK, and the scheme's feasibility and practicability are established. The health-zkIDM system proposed by [20] is a decentralized identity authentication system based on ZKP and blockchain technology. It enables patients to verify and identify their identities transparently in various health sectors and to interact with IDM providers while addressing the privacy-harming limitations of centralized IDMs. Chaincode implementation on the fabric demonstrates that the plan can produce throughputs greater than 400 TPs in Caliper.

In order to address issues with the openness of the blockchain network, which temporarily jeopardizes the privacy and validity of the voting content, [19] developed a smart contract voting system. Additionally, the four stages' execution process and associated algorithm were added to the suggested voting system, and the execution results took the form of a contract transaction. The cryptographic protocol and smart contract voting system can both be effectively provided by the smart contract voting system. [21] book covers a wide range of topics, with a focus on data security and privacy protection, including the internet of things (IOTs), intelligent manufacturing, finance, and health. By examining and contrasting current security countermeasures, the research focuses on security issues in blockchain technology that are specific to health and identifies six layers of security risks.

**3. Formulation of blockchain based secure data sharing scheme model for distributed VANET**

The proposed mathematical model composed of vehicular networks (Ordinary Node, Edge Node and Road side unit (RSU)) and Certificate Authority (CA) that is in charge of managing the key generation for all system components. The blockchain and zero knowledge proof (ZKP) will serve as the model's foundations.

On the basis of the consortium blockchain and the cryptographic tool ZKP, the data sharing scheme achieves authentication. The proposed model employs the subsequent procedures:

1. **System Initialization**: The cryptographic tools that are used by every CA are used in this step. Pairing operations are used by the CA for this.

According to effective bilinear map functions , the CA first selects two multiplication groups G1 and G2 of prime order p and p1, respectively.

Conversely, it picks some generators and and defines three collision-proof hashing techniques as:

Where, p is a prime

The CA then creates the ensuing key pairs as:

They are a pair of secret and public keys that are used to generate keys and deliver certificates for each network vehicle. The CA selects a secret key at random, , and computes the key pair for the CA as follows:

The pair of secret and public keys utilized for the audit of vehicular data is then provided by:

Similarly, generation, the decision-maker selects a secret key. and output its public key

Public parameters are output by the setup algorithm as follows:

params

The master key MK is given by:

MK =

The CA can deliver certificates and audit data using Equation 3.8.

The CA then uses its private key to sign the parameter params and publishes the tuple "" in the blockchain, which is maintained by the RSU vehicles.

1. **Vehicles and RSU key generation**: The CA must authenticate vehicles and RSU nodes to verify their identities. The CA will subsequently confirm and register the entity's (vehicles and RSU nodes) identity. Each authorized organization will then get its secret key, which enables it to authenticate and freely share raw data.

CA performs the following operations depending on the type of the entity:

1. Vehicle registration: The CA generates a pair of long-term public and secret keys as follows for each vehicle Vi:

Each time it shares data, the vehicle Vi will use the pair of keys to generate one-time pair of keys.

Furthermore, On the basis of the long-time public key, CA calculates the certificate Ci for Vi. For this model, the CA generates the pair of keys and the certificate for vehicle Vi as:

1. It computes a long-term public key and selects a long-term secret key at random, x1, x2 and Y1 = , Y2 = . It outputs the vehicles Vi ‘s pair of keys, from equation 3.9, it follows as:

Long-time secret key Long-time public key

1. Using the public and secret pair keys of the CA from equation 3.3 and the vehicles long time public key of Vi , the CA randomly pick some key v, h and employs its secret key. to figure . The CA sends the certificate to vehicle Vi
2. RSU Nodes Registration: The CA generates public and private keys (PKRSUi and SKRSUi, respectively) as well as the corresponding certificate Certi for each valid RSU node (RSUj). The public key PKRSUi is used to encrypt the raw data, and this certificate is used by entities to authenticate the node RSUj.
3. **Data Sharing**: According to the system model, vehicle Vi must first create a one-time pair of keys that are used to sign the data and provide a ZKP of its identity before it can communicate with an RSU edge node to share traffic data.

The following operations are performed by vehicle Vi for the above statement.

1. A pair of one-time keys is generated by:

The vehicle Vi picks a key at random , so that long time public key from equation 3.10 will computes one-time public key as:

Similarly, long-time secret key from equation 3.10 and one-time secret key is computed as:

Note: The data is shared under the pseudonym " key," and vehicle Vi must use the ZKP mechanism to prove that the data is accurate.

1. Generation of ZKPs: According to (Camenisch & Stadler, 1997), the vehicle Vi generates ZKP from the discrete logarithm problem, the known pseudonym and corresponding secret key as follows:
2. Random value V was picked and computes

was computed again.

1. finally computed and outputs

Furthermore, the vehicle Vi must submit a ZKP that demonstrates its long-term public key from equation 3.10 and its one-time public key given in equation 11.

Additionally, the vehicle needs to show that the public key has a current certificate Ci that was delivered by the CA.

The vehicle Vi runs the proof of knowledge as follows to construct the ZKP, taking the certificate Ci = (Qi, h, v) as an input, the public key, and audpk auditor public key.

1. It chooses at random and compute

1. It randomly picks and computes as:

1. Utilizing the Boneh-Lynn-Shacham signature scheme, vehicle Vi computes the data M's signature by hashing it as h = H(M), and outputs the signature as
2. Using timestamp as the data generator's time, the challenge is computed as

1. It computes the following values: ,
2. Vehicle Vi outputs the ZKP as follows:

Now,

**Data Uploading in Raw**

After the ZKP are calculated, the Vi vehicle sends a request to share the data M and obtain its certificate to a nearby RSU node in the vehicular edge network, let's say the node RSUjj. After receiving Certj, vehicle Vi used the public key PKRSUJ of the node RSUj to encrypt the data M and validate the signature of Certi. Then, the vehicle Vi generates the metadata, identifying and describing the data M, and containing enough details to enable any node to anonymously authenticate the data M. It includes the vehicle Vi's one-time public key , ZKPs , the list of data M topics, the timestamp of its generation, and the ZKPs.

The metadata record is explicitly organized as follows:

After encryption with the public key PKRSUj, the vehicle Vi will then send the shared data M with metadata as a record.

1. **Authentication Module**: RSU uses its private key SKRSUj to decrypt a *Recordi* it receives in order to recover the raw data M and any associated metadata.

It then completes the subsequent actions:

1. Verification of Signature: The node RSU examines the data M and the one-time public key after receiving as a signature. If this is the case, the subsequent steps of authentication are carried out; otherwise, the received record is deleted.
2. Checking the correctness of ZKP: The node RSU outputs True if are valid ZKP on the basis of the received ZKPs and the public parameters params.

**Putting the Model Solution into Practice as a Smart Contract**

In order to create a secure and dependable data sharing protocol in VANETs, the research makes use of smart contracts. The main implementation of the research scheme is carried out by a smart contract that is maintained by each broker. All brokers who are in charge of keeping the raw data M in storage execute this smart contract after it has been deployed on the blockchain. The sharing protocol's security can be increased through the use of smart contracts.

1. **Data Storage and Block generation Module**: Each RSU node acts as a data aggregator in this solution, collecting a set of data records periodically from nearby vehicles. Data storage and block generation module. In this study, we make the supposition that the information published is accurate and derived from reliable sources.

However, this study does not take into account how to manage trust in data sources and delivery methods. The RSU node RSUj extracts the associated metadata from each received record "Recordi"\_and adds it to a fresh transaction "." The public keys of all RSU brokers who are in charge of keeping each piece of data that belongs to one or more topics listed in the metadata are then added to this transaction.

Additionally, the transaction is structure as follows:

Whereas "BrockersListi"\_will verify and save both the raw data M and the transaction . Each broker on this list is in charge of at least one list called "Topics."

A consensus algorithm is used by the broker RSUj to publish the data M along with the transaction to all of the brokers in the list "BrockersListi" for validation and verification. It is impossible to alter this data after its validation using the consensus and authentication processes because multiple brokers in the network have a copy of it. Each RSU broker must validate the transaction metadata using the underlying consensus algorithm and certify its veracity. will be included in the blockchain copy of all RSU broker in the system transactions once it has been validated.

1. **Tracking Module**: When things go wrong, the CA may occasionally need to investigate the shared data's source to look for signs of system abuse. We suggest a method that enables the CA to monitor each entity's public key by carrying out the following actions:

1) Depending on the attribute , The CA calculates and stores the information in the blockchain's metadata. .

2) The CA computes Y1 to determine the vehicle that shared the data and a portion of the long-term public key associated with the metadata. who shared data, the CA computes .

The proposed model is created to offer a reliable and scalable model for data storage and sharing that safeguards the confidentiality of sensitive data while preserving high availability. As a result, it has satisfied [22] and [23] good and strong blockchain-based zero knowledge proof model for secure data sharing and storage for distributed VANET.

**3.1 Experimental Setup**

Table 3 in this study displays the minimal system configurations for the initial assessment and validation of the proposed model.

**Table 1.** Preliminary experimental parameters.

|  |  |
| --- | --- |
| Parameter | Value |
| *Hardware* |  |
| Processor | 11th Gen Intel® Core™ i3 – 1125G4 @ 2.00GHz 2.00GHz |
| RAM | 8.00 GB |
| Hard Disk Drive (HDD) | 1TB |
| System Type | 64-bit Operating System, x64-based processor |
| *Software* |  |
| Operating System | Windows 10 Home |
| Application programming Interface | Visual Studio Code 18 |
| Traditional AES-256, base64code, SHA-1 |  |

**3.2 Data Collection**

Transportation datasets will be collected from Georgia Tech Library repository (https://www.fhwa.dot.gov/policyinformation/travel\_monitoring/tvt.cfm?CFID=204754188&CFTOKEN=24b7b7f820ee50e6-D19608D7-C420-C210-3B0984BD35EF1C66) for Travel monitoring. The pre-processing was carried out on various sensor datasets on Microsoft Excel 2017 version for removal of redundancy and reorganization.

This study will choose synthetic data for validation of the proposed model for cost reduction and efficiency. Similar synthetic data was deployed in health system scenario in [17]. The integration of blockchain-based for VANETs will provides reliable and secure data storage and sharing.

**Set Metrics**

1. Encryption time
2. Decryption time
3. Reliability
4. Accuracy
5. Availability

**4. Results and Discussions**

4.1 **Results**

This section covers the presentation of findings in tables as well as summary and interpretation on `findings with regard to the blockchain key generation. Table 2 below illustrates summary of key generation results using several messages (m) to generates cyphertext, cipher size and execution time.

**Table 2:** Summary of Model Validation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S/n** | **Data\_Experiment\_2** | **Proposed scheme** | **message size** | **ciphertext size** | **Encryption time (ms)** |
| 1. | 'gnfuv-temp-exp1-55d487b85b-5dmwq' | 10000:5b42403465323531353466:3  ce6e4caa0c2bb9eaa8604186a0fd3e4  6cc62453321db168906a45a4a61595  cf5404cebe32e97a24d14c8e2929f2c  e7ebc9492a2d549c1723f6678b46cd  1aa13 | 33 | 157 | 26373 |
| 2. | 'gnfuv-temp-exp1-55d487b85b-2648d' | 10000:5b42403465323531353466:27  b466d41a58e28375a6486de4f24edc  3478f44965f19b8dca4b60dcaac8e1cf  5b5f7ea4e7cc7cbe0c00ebc60c5b8b6f  044063d2f21356f721a2dae62828c522 | 33 | 157 | 27460 |
| 3. | 'gnfuv-temp-exp1-55d487b85b-t2rkn' | 10000:5b42403465323531353466:394  2e9322cfd4ce107553e227dbc350bf66  7e8b6d8dc9fc82039b8d235a87c5b3a3  e169a3ba72946815f18a7e28775b735  505fe108ca6242eb8f68fd4504ee09 | 33 | 157 | 28620 |
| 4. | 'gnfuv-temp-exp1-55d487b85b-b9wx5' | 10000:5b42403465323531353466:b1  817443067bd9cfc3a295bb59b4288e4  ddd2d61ed782302d81bcd71e129d05  26de589edb29e696a063eb39ff02a5d  3433e12949d164d27d51dd0b878a6b  6231 | 33 | 157 | 28162 |
|  | **Data\_Experiment\_1** |  |  |  | **Decryption**  **Time (ms)** |
| 1. | 'gnfuv-temp-exp1-55d487b85b-5g2xh' | 10000:5b42403465323531353466:d8  73745e8ce455a8255a39bf35fe5fd0d  162c0d02e8aeee662def3de85f6750f8  289424b31d11512a104d96eb87240e  5f364e91c1d317a8018ba6a10414c60f | 33 | 156 | 26865 |
| 2. | 'gnfuv-temp-exp1-55d487b85b-2bl8b' | 10000:5b42403465323531353466:b8  bf73584882adaa164b14a72129c2916  b6fa9b51a633ffa6cf199b30398c5ac8  d88acf1ed5b5e87f1f38f98ed05fc50a  dc80915997b401b62ac7c2dafec2afd | 33 | 157 | 27196 |
| 3. | 'gnfuv-temp-exp1-55d487b85b-2msrd' | 10000:5b42403465323531353466:c4  e14e577c526cdf3d6efacb53e624978  283384f08208c871a8ccf3bf4352f2fb  ca5e763f1194baf34c9ff147de8d0ed  a6363e89046c3986a202ce4eeb6795  99 | 33 | 157 | 28875 |
| 4. | 'gnfuv-temp-exp1-55d487b85b-5dmwq' | 10000:5b42403465323531353466:3c  e6e4caa0c2bb9eaa8604186a0fd3e46  cc62453321db168906a45a4a61595cf  5404cebe32e97a24d14c8e2929f2ce7  ebc9492a2d549c1723f6678b46cd1aa  13 | 33 | 157 | 28866 |
|  |  |  |  |  |  |
|  |  | **ADVANCED ENCRYPTION STANDARD (AES)** |  |  |  |
|  | **Data\_Experiment\_2** |  |  |  | **Encryption time (ms)** |
| 1. | 'gnfuv-temp-exp1-55d487b85b-5dmwq' | dt2ETHnEx1aMFokWa6+csmPczfvfivR  IbZGdpmDp0OD4UW00ssPMcCJRaaU  GpesQ | 33 | 64 | 1952 |
| 2. | 'gnfuv-temp-exp1-55d487b85b-2648d' | olddJma7QlZDrNQob+mVHJpCK1ks/d  jyUHlB2E8IIq0U/NzmSkNM64jJQ/rjIA  zd | 33 | 64 | 2086 |
| 3. | 'gnfuv-temp-exp1-55d487b85b-t2rkn' | Y9CBurJq3DCKNCV+YvD8Xd6Tn/sMn  nc1qCwMdBefWXN6vbBJcZ8rqz8H+  dhcarla | 33 | 64 | 1866 |
| 4. | 'gnfuv-temp-exp1-55d487b85b-b9wx5' | hYTG9DYQrRLbw70ZQGbK11CI0vnb  9vn6M5UJuuCJy3o7MJ2PLSc0CqNr  Jgl4L/nN | 33 | 64 | 1768 |
|  | **Data\_Experiment\_1** |  |  |  | **Decryption time (ms)** |
| 1 | 'gnfuv-temp-exp1-55d487b85b-5g2xh' | iBWWI6CyCu2D6UaqTpxxhBpluUwj  1/jkbyGSWV2vSHz1AFVSo7u2jXPT1  oFHIBcJ | 33 | 64 | 2126 |
| 2. | 'gnfuv-temp-exp1-55d487b85b-2bl8b' | t9pGTZsNcpKapS72OmSRsnvkidiuh  NMAojt3lDJiYOwT5qfvmGyd67yV/  c4+owCc | 33 | 64 | 2527 |
| 3. | 'gnfuv-temp-exp1-55d487b85b-2msrd' | dCRKGAdC7NplSjr0qQL77ZO54RCq  kJr3ZIoKEcHKvjWUNvtYdQI939QZV  rLJ12ag | 33 | 64 | 4586 |
| 4. | 'gnfuv-temp-exp1-55d487b85b-5dmwq' | dt2ETHnEx1aMFokWa6+csmPczfvfi  vRIbZGdpmDp0OD4UW00ssPMcCJ  RaaUGpesQ | 33 | 64 | 7817 |

In Table 2, both the proposed scheme and the Advanced encryption standard (AES) use the same message size (m). Nevertheless, the US government recognizes and suggests using the AES encryption standard. The maximum key length permitted by AES is 256 bits. However, the encryption and decryption standard's effectiveness were tested using the same message size.

**4.2 Data Presentation**

From the model validation in figure 1 we observed that for message sizes (m), the ciphertext size for both data experiment \_­2 and 1 are the same except for 'gnfuv-temp-exp1-55d487b85b-5g2xh' which generate ciphertext size 156bits with lowest decryption time of 26,865ms. In overall, submission the proposed scheme has the larger encryption and decryption time than the AES in comparison. Similarly, AES generates the same ciphertext although for both encryption and decryption time, the decryption time takes longer time to decrypt than to encrypt as shown in figure 2.

**Figure 1:** Model Validation Chart

Advanced encryption standard chart in figure 2 shows that AES takes longer time todecrypt than to encrypt message size (m), the line graph shows a projection in decrypting a message.

**Figure 2:** Advanced Encryption Standard

We deduced that; encryption time is not determine by numbers of message sizes. However, larger the message sizes, determine efficient security of the key sharing. Figure 3 below shows encryption and decryption time graph for the proposed scheme.

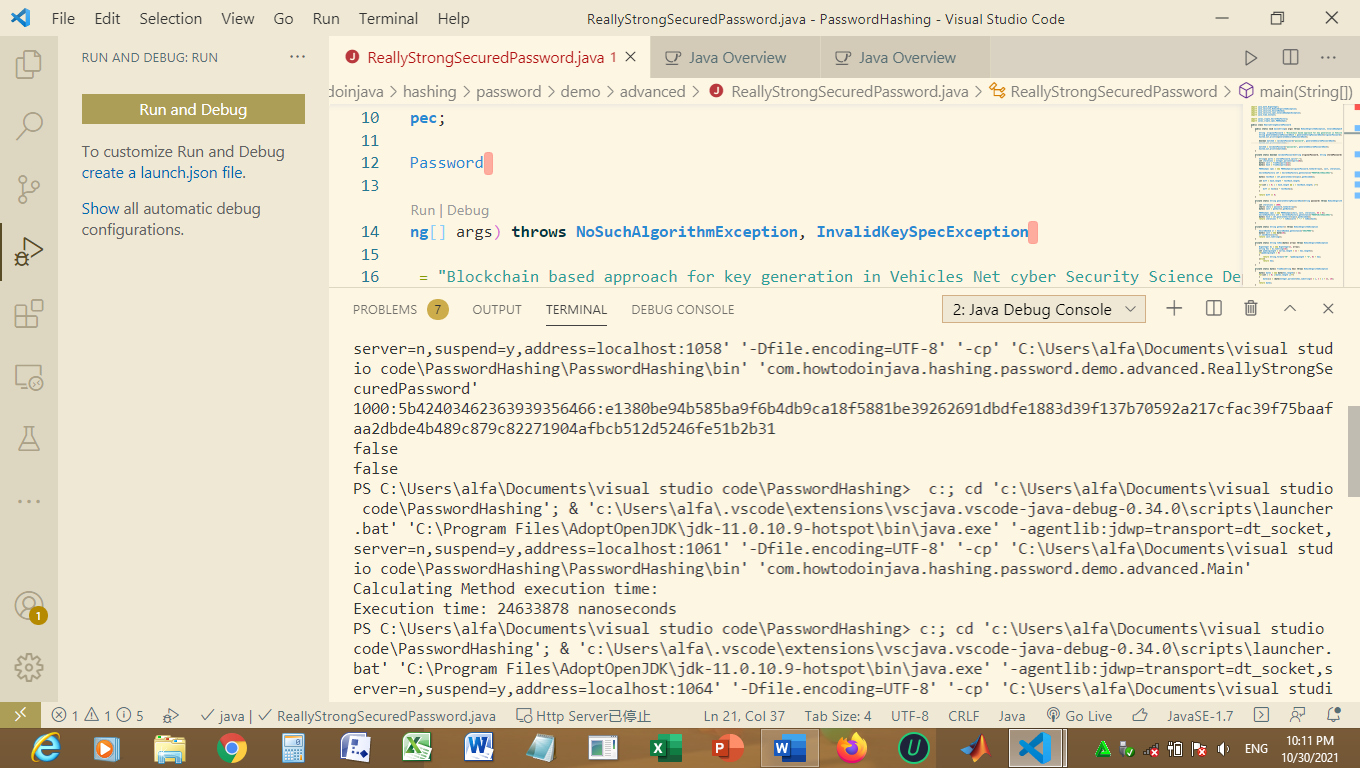
**Figure 3:** Proposed scheme encryption and decryption time graph

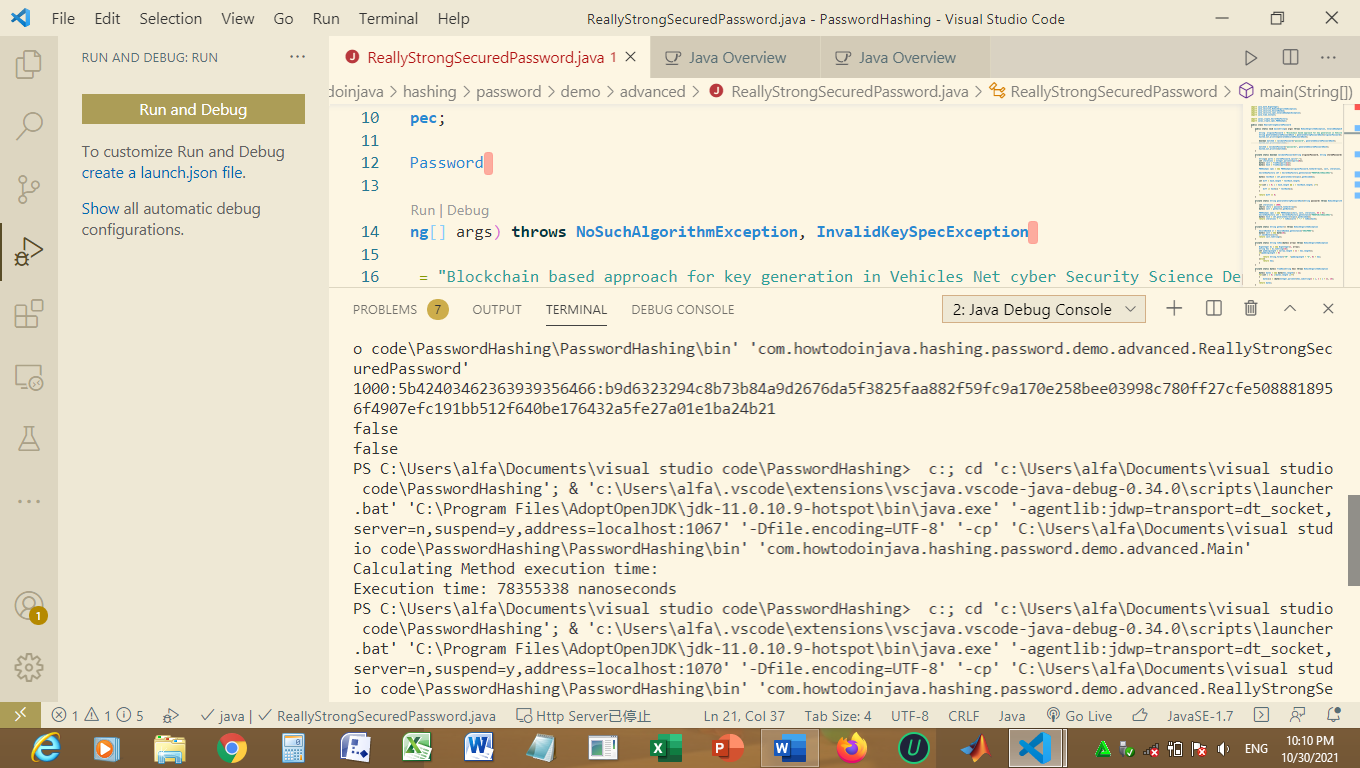
The proposed scheme time graph shows the geometric progression in both encryption and decryption time, we observed little decrease in encryption between 28,620ms and 28,162ms. However, the linear graph is not affected, Additionally, the model validation complies with a good and reliable blockchain-based zero knowledge proof model for distributed VANET secure data sharing and storage. Below is AES encryption and decryption time graph.

**Figure 4:** AES encryption and decryption time graph

We observed from figure 4 that decrypting a AES message using the same message size takes a longer time than encrypting as shown in the AES time graph.

The interface of the validation model is presented in Figure 5. it shows the processes of key generation.





**Figure 5:** Model Validation Interface

**5. Conclusion**

In this study, we proposed a mathematical model made up of vehicular networks, including Ordinary Node, Edge Node, and Road Side Unit (RSU) networks, as well as a Certificate Authority (CA), which is in charge of overseeing the key generation for all system components. The model is based on the blockchain and zero knowledge proof (ZKP).

In this solution, each RSU node performs the role of a data aggregator by routinely gathering a set of data records from nearby vehicles. Block generation and data storage module. In order to establish a secure, dependable data sharing protocol and to assume that the information published is accurate and derived from reliable sources, the study uses smart contracts. Vehicles and RSU nodes must be authenticated by the CA in order to confirm their identities. The CA will then verify and register the identity of the entity (vehicles and RSU nodes). This study, however, does not address the issue of managing trust in data sources and delivery mechanisms.

The proposed model aims to provide a scalable, secure, and reliable model for data storage and sharing that maintains high availability while protecting the confidentiality of sensitive data. As a result, the proposed model validation shows that the model performed better than Advanced encryption standard in term of ciphertext size, encryption time and decryption time and it satisfies the good and robust blockchain-based zero knowledge proof model for secure data sharing and storage for distributed VANET proposed by [22] and [23].

**REFERENCES**

[1] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, “Internet of vehicles in big data era,” IEEE/CAA Journal of Automatica Sinica, vol. 5, no. 1, pp. 19–35, 2018.

[2] J. Ni, A. Zhang, X. Lin, and X. S. Shen, “Security, privacy, and fairness in fog-based vehicular crowdsensing,” IEEE Communications Magazine, vol. 55, no. 6, pp. 146–152, 2017.

[3] Z. Su, Y. Hui, and Q. Yang, “The next generation vehicular networks: A content-centric framework,” IEEE Wireless Communications, vol. 24, no. 1, pp. 60–66, 2017.

[4] Q. Yang, B. Zhu, and S. Wu, “An architecture of cloud-assisted information dissemination in vehicular networks,” IEEE Access, vol. 4, pp. 2764–2770, 2016.

[5] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, “Exploring mobile edge computing for 5g-enabled software defined vehicular networks,” IEEE Wireless Communications, vol. 24, no. 6, pp. 55–63, 2017.

[7] Firdaus, M.; Rhee, K.H. Empowering Blockchain for Secure Data Storing in Industrial IoT. In Proceedings of the Korea Information Processing Society Conference, Seoul, Korea, 29–30 May 2020; pp. 231–234.

[8] Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. 2018, 19, 2204–2220.

[9] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 September 2020)

[10] Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors 2019, 19, 4954.

[11] Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access 2019, 7, 56656–56666.

[12] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell. World of empowered iot users. In IEEE 1st International Conference on Internetof-Things Design and Implementation, pages 13–24, 2016.

[13] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang. Bbds: Blockchain based data sharing for electronic medical records in cloud environments. Information, 8(2):44, 2017.

[14] D. Augot, H. Chabanne, O. Clemot, and W. George, “Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain,” in Proceedings - 2017 15th Annual Conference on Privacy, Security and Trust, PST 2017, 2018.

[15] E. O. Blass and F. Kerschbaum, “Strain: A secure auction for blockchains,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018.

[16] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2018. Available online: Https://bitcoin.org/ bitcoin.pdf (accessed on 18 November 2019).

[17] Dahmen, J., & Cook, D. (2019). *SynSys : A Synthetic Data Generation System for Healthcare Applications*. 1–11. <https://doi.org/10.3390/s19051181>

[18] Fan, Y., Xu, B., Zhang, L., Song, J., Zomaya, A., & Li, K. C. (2023). Validating the integrity of Convolutional Neural Network predictions based on Zero-Knowledge Proof. Information Sciences.

[19] YIN Hong-jian, ZHU Yan, WANG Jing, GUO Guang-lai, CHEN E. Design and implementation of a smart-contract voting system based on zero-knowledge proof[J]. Chinese Journal of Engineering, 2023, 45(4): 632-642. doi: 10.13374/j.issn2095-9389.2022.07.07.001

[20] Bai, T.; Hu, Y.; He, J.; Fan, H.; An, Z. Health-zkIDM: A Healthcare Identity System Based on Fabric Blockchain and Zero-Knowledge Proof. Sensors 2022, 22, 7716. https://doi.org/10.3390/s22207716

[21] Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. Electronics, 12(3), 546.

[22] Al-Aswad, H., Hasan, H., Elmedany, W.M., Ali, M., & Balakrishna, C. (2019). Towards a Blockchain-Based Zero-Knowledge Model for Secure Data Sharing and Access. 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 76-81.

[23] Hafid, A., Hafid, A. S., & Samih, M. (2019). New mathematical model to analyze security of sharding-based blockchain protocols. *IEEE Access*, *7*, 185447-185457.