FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 7 No. 3, June, 2023, pp 45 - 54
DOI: https://doi.org/10.33003/fjs-2023-0703-1786

BLOCKCHAIN-BASED ZERO KNOWLEDGE PROOF MODEL FOR SECURE DATA SHARING SCHEME IN A DISTRIBUTED VEHICULAR NETWORKS

[*1]Muhammad Umar Majigi, [1]Ismaila Idris, [2]Shafii M. Abdulhamid, [1]Andrew Anogie Uduimoh

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.
[2]Department of Cybersecurity and Networking. Community College of Qatar Doha, Qatar

*Corresponding authors' email: majigiumar1@gmail.com

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 157 bits, 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 the Advanced encryption standard in terms 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

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 (Xu *et al,*. 2018). Furthermore, data of common interest are share and collected by vehicles (Ni *et al.,* 2017), (Su *et al.,* 2017). 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 (Yang *et al.,* 2016). 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 is locally relevant data for vehicles with spatial scope and overt lifetime of utility which requires location awareness and low latency for vehicular data sharing (Ni *et al.,* 2017). 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 (Ni *et al.,* 2017), (Huang *et al.,* 2017). 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 (Firdaus and Rhee, 2020).

The data sharing in a VANET contain critical data of users which make data privacy increasable significant in the areas of data storage (Firdaus *et al.,* 2020). 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 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 (Li *et al.,* 2018). Thus, the incentives mechanism nature is leveraged to encourage vehicles and users to share and store their data while evaluating the trustworthiness of data in VANET.

Since Nakamoto introduced Bitcoin (Nakamoto, 2020), in the past ten years blockchain has gained much popularity as an emerging technology to provide better security for data sharing among many parties without an intermediary. Blockchain is known as a suitable solution that addresses the privacy security issue (Khan *et al.,* 2019), in the last years when Nakamoto introduced Bitcoin (Nakamoto, 2020), (Xie *et al.,* 2019) blockchain gained much popularity as an emerging technology in providing better security on data sharing without an intermediary, which can simplify a trusted, secure, trusted and decentralized smart transportation system.

In 2008 Satoshi Nakamoto introduces blockchain technology (Nakamoto, 2019) to provide the best security, establish trust entities and ensure privacy. With the increasing number of records stored in the form of blocks, when joined together in 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 the block is generated, transaction data in the form of Merkle root tree and nonce, which is an arbitrary number used for the mining process.

The research has established the following contributions:

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

Related Work

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

A decentralized solution was proposed by (Hashemi *et al.,* 2016) 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, (Xia *et al.,* 2017) 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.

(Arif *et al.,* 2019) discussed security and privacy concerns while presenting the intelligent transportation systems to VANET. They discussed the effectiveness of the VANET and cloud computing as well as a solution to privacy and security issues. Additionally, current VANET issues are discussed.

Augot *et al.,* (2017) built an 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. (Blass *et al.*, 2018) Another tool for making secure auction systems is interactive implementation, which only requires four miner confirmations. 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, (Fan *et al.,* 2023) 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 (Bai *et al.*, 2022) 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 vehicular computing and networks, (Jiawen *et al.,* 2019) presented a secure P2P data sharing system. To achieve secure and effective data storage and data sharing, a combination of blockchain and smart contract technologies was used. These technologies effectively stop unauthorized sharing of used data. Strong computing and vast storage resources are made available by vehicular edge computing and networks (VECNETs). The use of roadside units as vehicular edge computing servers, however, raises serious security and privacy concerns because they cannot be completely trusted.

In order to address issues with the openness of the blockchain network, which temporarily jeopardizes the privacy and validity of the voting content, (Yin *et al.,* 2023) 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. (Wenhua *et al.,* 2023) The Internet of Things (IOTs), intelligent manufacturing, finance, and health are just a few of the many subjects covered in the research paper, which also places a strong emphasis on data security and privacy protection. The research focuses on security issues in blockchain technology that are particular to health and identifies six layers of security risks by comparing and contrasting current security countermeasures.

METHODOLOGY

Formulation Of Blockchain-Based Secure Data Sharing Scheme Model For Distributed Vanet

The proposed mathematical model is composed of vehicular networks (Ordinary Node, Edge Node and Road side unit (RSU)) and a 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 $\hat{e}$, the CA first selects two multiplication groups G_1 and G_2 of prime order p and p1, respectively.

$$\hat{e}: G_1 \, X \, G_1 \rightarrow G_2 \quad (1)$$

Conversely, it picks some generators $g_1 \in G_1$ and $g_2 \in G_2$ and defines three collision-proof hashing techniques as:

$$\begin{cases} H_1: \{0,1\}^* \rightarrow Z_p \\ H_2: G_1 \rightarrow Z_p \\ H : \{0,1\}^* \rightarrow \{0,1\}^m \end{cases} \quad (2)$$

Where, p is a prime

The CA then creates the ensuing key pairs as:

$$CA_{key} = (Ca_{sk}, Ca_{pk}) \quad (3)$$

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, $\beta \in Z_p$, and computes the key pair CA_{key} for the CA as follows:

$$Ca_{sk} = \beta, Ca_{pk} = g_1^{\beta} \quad (4)$$

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

$Aud_{key} = (aud_{sk}, aud_{pk})$ (5)

Similarly, CA_{key} generation, the decision-maker selects a secret key. $aud_{sk} \in Z_p$ and output its public key

$aud_{pk} = g_1^{aud}sk$ (6)

Public parameters are output by the setup algorithm as follows:

Param = $\{g_1, g_{2,} e, Ca_{pk}, aud_{pk,} H_{1,} H_{2,} H\}$ (7)

The master key MK is given by:

MK = (Ca_{sk}, aud_{sk}) (8)

The CA can deliver certificates and audit data using Equation 8.

The CA then uses its private key to sign the parameter params and publishes the tuple " $< params, \sigma ca_{sk}(params), Ca_{pk} >$ " in the blockchain, which is maintained by the RSU vehicles.

2. **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:

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

$(T_{pk,i}, T_{sk,i})$ (9)

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 C_i for V_i. For this model, the CA generates the pair of keys and the certificate for vehicle V_i as:

i. It computes a long-term public key and selects a long-term secret key at random, x_1, $x_2 \in Z_p$ and $Y_1 = g_1^{x1}$, $Y_2 = g_2^{x2}$. It outputs the vehicles V_i 's pair of keys, from equation 9, it follows as:

$$\underbrace{\left(T_{sk,i} = (x1, x2),\right.}_{\text{Long-time secret key}} \underbrace{\left. T_{pk,i} = (Y_1, Y_2)\right)}_{\text{Long-time public key}} \quad (10)$$

ii. Using the public and secret pair keys of the CA from equation 3 (Ca_{pk}, Ca_{sk}) and the vehicles long time public key of V_i $T_{pk,i} = (Y_1, Y_2)$, the CA randomly pick some key v, h $\in Z_p$ and employs its secret key. $Ca_{sk} = \beta$ to figure $Q_i = (g_1.Y_1.g_1^v)^{.1/\beta+h}$. The CA sends the certificate $C_i = (Q_i, h, v)$ to vehicle V_i

b. RSU Nodes Registration: The CA generates public and private keys (PK_{RSUi} and SK_{RSUi}, respectively) as well as the corresponding certificate $Cert_i$ for each valid RSU node (RSU_j). The public key PK_{RSUi} is used to encrypt the raw data, and this certificate is used by entities to authenticate the node RSU_j.

3. **Data Sharing**: According to the system model, vehicle V_i 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.

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

$$\delta tk_i = \left(\delta tpk_i, \overbrace{\delta tsk_i}^{One\ time\ secret\ key}\right) \quad (11)$$

The vehicle V_i picks a key at random $f_d \in Z_p$, so that long time public key from equation 10 will compute one-time public key as:

$$\left(F = g_1^{fd}, \delta tpk_i = Y_1.g_1^{H2\left(Y_2^{fd}\right)}\right) \quad (12)$$

Similarly, long-time secret key from equation 10 and one-time secret key is computed as:

$\delta tsk_i = x_1 + H_1(F)$ (13)

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

b. Generation of ZKPs: According to (Camenisch & Stadler, 1997), the vehicle V_i generates ZKP from the discrete logarithm problem, the known pseudonym δtsk_i and corresponding secret key δtsk_i as follows:

i. Random value V $\in Z_p^*$ was picked and computes t $= g_1^{vi}, f = H_1(g_1 \parallel \delta tsk_i \parallel t)$ was computed again.

ii. $M = g_1^{v-f.\delta tsk_i}$ finally computed and outputs $\pi_{\delta tsk} = (\delta tsk_i,\ t, M)$

Furthermore, the vehicle V_i must submit a ZKP that demonstrates its long-term public key $T_{pk,i}$ from equation 10 and its one-time public key δtsk_i given in equation 11.

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

The vehicle V_i runs the proof of knowledge as follows to construct the ZKP, taking the certificate C_i = (Q_i, h, v) as an input, the public key, and aud_{pk} auditor public key.

i. It chooses at random $f_{cert} \in Z_p$ and compute $C_f = \left(C_{cert} = Y_i.aud_{pk}^{fcert}, R_{cert} = g_1^{fcert}\right)$

ii. It randomly picks $q, f_{1,} f_2, f_{3,}\ f_4 \in Z_p$ and computes as: $\varphi = Q_i^q, R_c = \hat{e}\left(g_1\left(h_{cert}g_1^{f2}\varphi^{-f3}aud_{pk}^{-f4}, g_2\right)\right)$

iii. Utilizing the Boneh-Lynn-Shacham signature scheme, vehicle V_i computes the data M's signature by hashing it as h = H(M), and outputs the signature as $\delta = h^{\delta tski}$.

iv. Using timestamp as the data generator's time, the challenge is computed as $C = H_1\left(timestamp \parallel h \parallel C_f \parallel \varphi \parallel R_c\right)$.

v. It computes the following values: $Z_1 = f_1 + c.q$, $Z_2 = f_2 + c.q.v$, $Z_3 = f_3 + c.h$, $Z_4 = f_4 + c.f_{cert}.q$

vi. Vehicle V_i outputs the ZKP as follows: $\pi_i = (C, \varphi, Z_1, Z_2, Z_3, Z_4)$

Now,

Data Uploading in Raw

After the ZKP are calculated, the V_i 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 RSU_{jj}. After receiving $Cert_j$, vehicle V_i used the public key PK_{RSUJ} of the node RSU_j to encrypt the data M and validate the signature of $Cert_i$. Then, the vehicle V_i 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 V_i's one-time public key δtsk_i, ZKPs $\pi_{\delta tsk}$ and π_i, the list of data M topics, the timestamp of its generation, and the ZKPs.

The metadata record is explicitly organized as follows:

$metadata = (timestamp \parallel \delta tsk_i \parallel \pi_{\delta tsk} \parallel \pi_i \parallel topics \parallel \delta)$ (14)

After encryption with the public key PK_{RSUj}, the vehicle V_i will then send the shared data M with metadata as a record.

4. **Authentication Module**: RSU uses its private key SK_{RSUj} to decrypt a $Record_i$ it receives in order to recover the raw data M and any associated metadata.

It then completes the subsequent actions:

i. Verification of Signature: The node RSU examines the data M and the one-time public key δtsk_i after receiving δ as a signature $\hat{e}(H(M), \delta tsk_i) = \hat{e}(\delta, g_1)(H(M)\ is\ the\ hash\ of\ M)$ If this is the case, the subsequent steps of authentication are carried out; otherwise, the received record is deleted.

ii. Checking the correctness of ZKP: The node RSU outputs True if $\pi_{\delta tsk}\ and\ \pi_i$ are valid ZKP on the basis of the received ZKPs $\pi_{\delta tsk}\ and\ \pi_i$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.

5. 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 RSU_j extracts the associated metadata from each received record "$Record_i$"_and adds it to a fresh transaction " tx_i." 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 tx_i transaction is structure as follows:

$tx_i = (metadata \parallel \{PK_{RSUj}, RSU_j \in BrockersList_i\})$ (15)

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

A consensus algorithm is used by the broker RSU_j to publish the data M along with the transaction $tx_i$to all of the brokers in the list "$BrockersList_i$" 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 tx_i metadata using the underlying consensus algorithm and certify its veracity. tx_i will be included in the blockchain copy of all RSU broker in the system transactions once it has been validated.

5. **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 $C_r = (C_{cert} = Y_1.aud_{pk}^{rcert}, B_{cert} = g_1^{rcert})$, The CA calculates and stores the information in the blockchain's metadata. $B'_{cert} = B_{cert}^{audsk} = aud_{pk}^{rcert}$.

2) The CA computes Y_1 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 $Y1 = C_{cert} / B'_{cert}$.

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 (Al-Aswad *et al.,* 2019) and (Hafid *et al.,* 2019) good and strong blockchain-based zero knowledge proof model for secure data sharing and storage for distributed VANET.

Experimental Setup

Table 1 shows 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	

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.

For the purpose of validating the suggested model for cost-reduction and efficiency, this study will use synthetic data. Similar synthetic data was used in (Dahmen & Cook, 2019) in a scenario involving a health system. Blockchain-based

VANET integration will offer dependable and secure data sharing and storage.

Set Metrics

i. Encryption time
ii. Decryption time
iii. Reliability
iv. Accuracy
v. Availability

This paper uses smart contracts to facilitate efficient, dependable, and secure data sharing. A smart contract is a piece of code stored on blockchains that enables the automation of multi-step processes that cannot be changed or stopped due to their distributed nature. Because of this, the use of smart contracts may enhance the vehicular blockchain's reliability, efficiency and security. On the vehicular blockchain, smart contracts are implemented to support secure and decentralized data sharing.

RESULTS AND DISCUSSIONS

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'	10000:5b424034653235313534 66:3ce6e4caa0c2bb9eaa8604186a0fd3e46cc62453321db168906a45a4a61595cf5404cebe32e97a24d14c8e2929f2ce7ebc9492a2d549c1723f6678b46cd1aa13	33	157	26373
2.	'gnfuv-temp-exp1-55d487b85b-2648d'	10000:5b424034653235313534 66:27b466d41a58e28375a6486de4f24edc3478f44965f19b8dca4b60dcaac8e1cf5b5f7ea4e7cc7cbe0c00ebc60c5b8b6f044063d2f21356f721a2dae62828c522	33	157	27460
3.	'gnfuv-temp-exp1-55d487b85b-t2rkn'	10000:5b424034653235313534 66:3942e9322cfd4ce107553e227dbc350bf667e8b6d8dc9fc82039b8d235a87c5b3a3e169a3ba72946815f18a7e28775b735505fe108ca6242eb8f68fd4504ee09	33	157	28620
4.	'gnfuv-temp-exp1-55d487b85b-b9wx5'	10000:5b424034653235313534 66:b1817443067bd9cfc3a295bb59b4288e4ddd2d61ed782302d81bcd71e129d0526de589edb29e696a063eb39ff02a5d3433e12949d164d27d51dd0b878a6b6231	33	157	28162
	Data_Experiment_1				**Decryption Time (ms)**
1.	'gnfuv-temp-exp1-55d487b85b-5g2xh'	10000:5b424034653235313534 66:d873745e8ce455a8255a39bf35fe5fd0d162c0d02e8aeee662def3de85f6750f8289424b31d11512a104d96eb87240e5f364e91c1d317a8018ba6a10414c60f	33	156	26865
2.	'gnfuv-temp-exp1-55d487b85b-2bl8b'	10000:5b424034653235313534 66:b8bf73584882adaa164b14a72129c2916b6fa9b51a633ffa6cf199b30398c5ac8d88acf1ed5b5e87f1f38f98ed05fc50adc80915997b401b62ac7c2dafec2afd	33	157	27196
3.	'gnfuv-temp-exp1-55d487b85b-2msrd'	10000:5b424034653235313534 66:c4e14e577c526cdf3d6efacb53e624978283384f08208c871a8ccf3bf4352f2fbca5e763f1194baf34c9ff147de8d0eda6363e89046c3986a202ce4eeb679599	33	157	28875
4.	'gnfuv-temp-exp1-55d487b85b-5dmwq'	10000:5b424034653235313534 66:3ce6e4caa0c2bb9eaa8604186a0fd3e46	33	157	28866

		cc62453321db168906a45a4a61595cf5404cebe32e97a24d14c8e2929f2ce7ebc9492a2d549c1723f6678b46cd1aa13			
		ADVANCED ENCRYPTION STANDARD (AES)			
	Data_Experiment_2				**Encryption time (ms)**
1.	'gnfuv-temp-exp1-55d487b85b-5dmwq'	dt2ETHnEx1aMFokWa6+csmPczfvfivRIbZGdpmDp0OD4UW00ssPMcCJRaaUGpesQ	33	64	1952
2.	'gnfuv-temp-exp1-55d487b85b-2648d'	olddJma7QlZDrNQob+mVHJpCK1ks/djyUHlB2E8IIq0U/NzmSkNM64jJQ/rjIAzd	33	64	2086
3.	'gnfuv-temp-exp1-55d487b85b-t2rkn'	Y9CBurJq3DCKNCV+YvD8Xd6Tn/sMnnc1qCwMdBefWXN6vbBJcZ8rqz8H+dhcarla	33	64	1866
4.	'gnfuv-temp-exp1-55d487b85b-b9wx5'	hYTG9DYQrRLbw70ZQGbK11CI0vnb9vn6M5UJuuCJy3o7MJ2PLSc0CqNrJgl4L/nN	33	64	1768
	Data_Experiment_1				**Decryption time (ms)**
1	'gnfuv-temp-exp1-55d487b85b-5g2xh'	iBWWI6CyCu2D6UaqTpxxhBpluUwj1/jkbyGSWV2vSHz1AFVSo7u2jXPT1oFHIBcJ	33	64	2126
2.	'gnfuv-temp-exp1-55d487b85b-2bl8b'	t9pGTZsNcpKapS72OmSRsnvkidiuhNMAojt3lDJiYOwT5qfvmGyd67yV/c4+owCc	33	64	2527
3.	'gnfuv-temp-exp1-55d487b85b-2msrd'	dCRKGAdC7NplSjr0qQL77ZO54RCqkJr3ZIoKEcHKvjWUNvtYdQI939QZVrLJ12ag	33	64	4586
4.	'gnfuv-temp-exp1-55d487b85b-5dmwq'	dt2ETHnEx1aMFokWa6+csmPczfvfivRIbZGdpmDp0OD4UW00ssPMcCJRaaUGpesQ	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.

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.

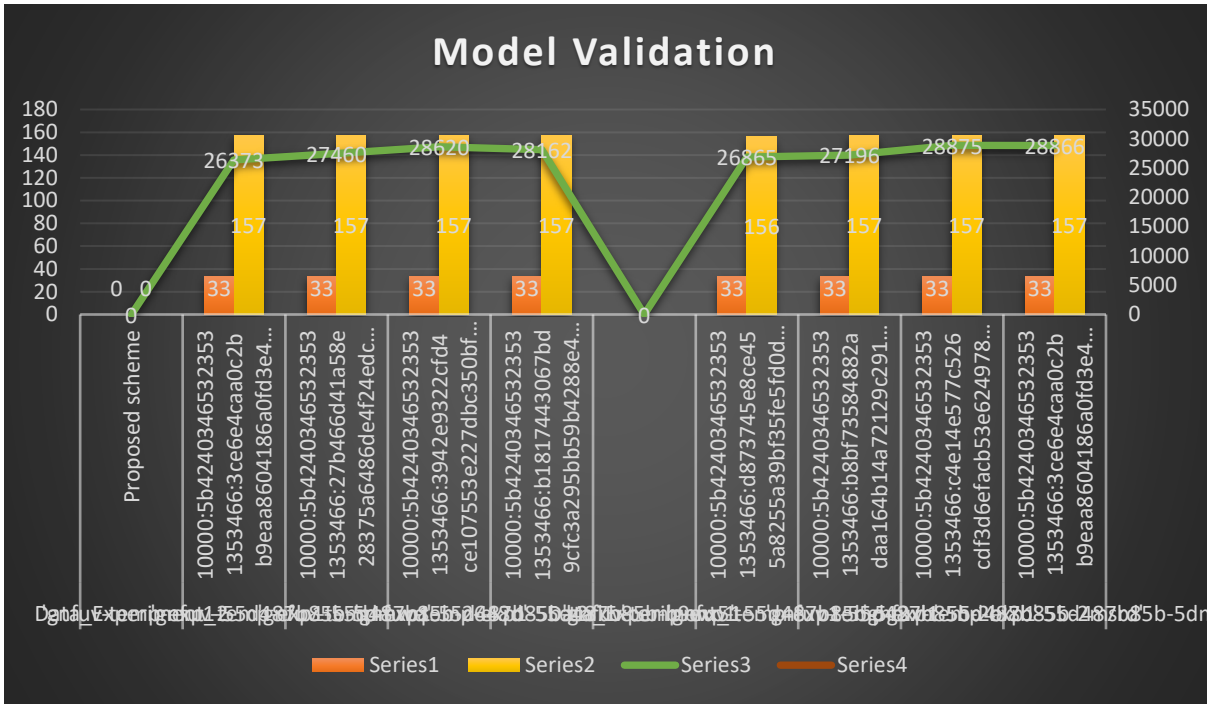

Figure 1**:** Model Validation Chart

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

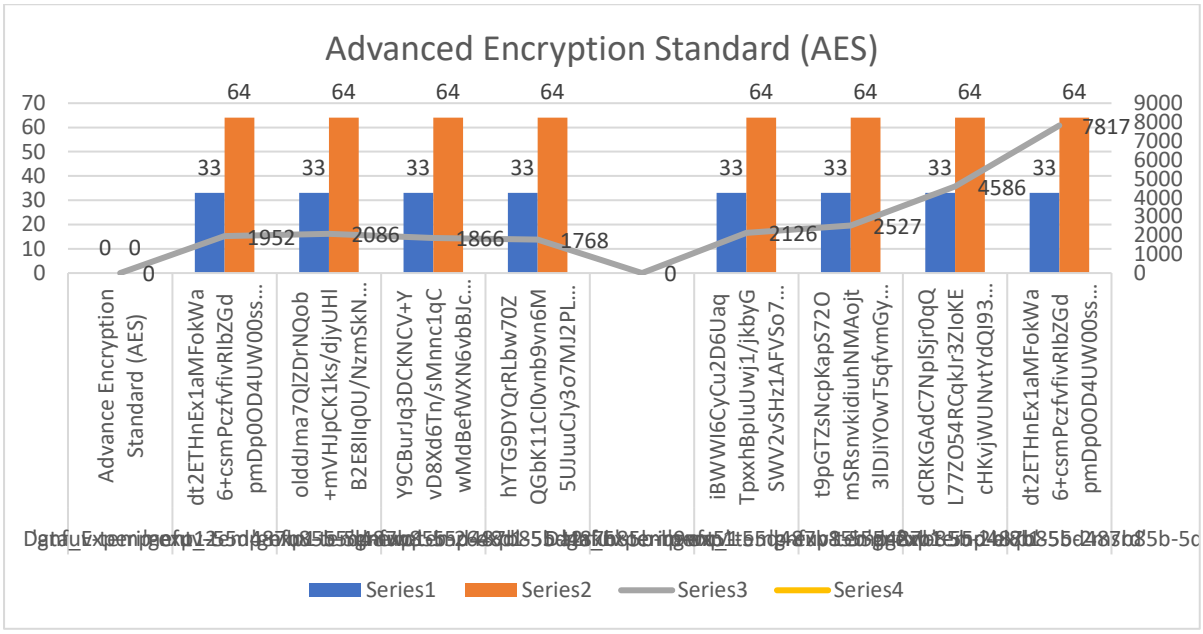

Figure 2: Advanced Encryption Standard

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

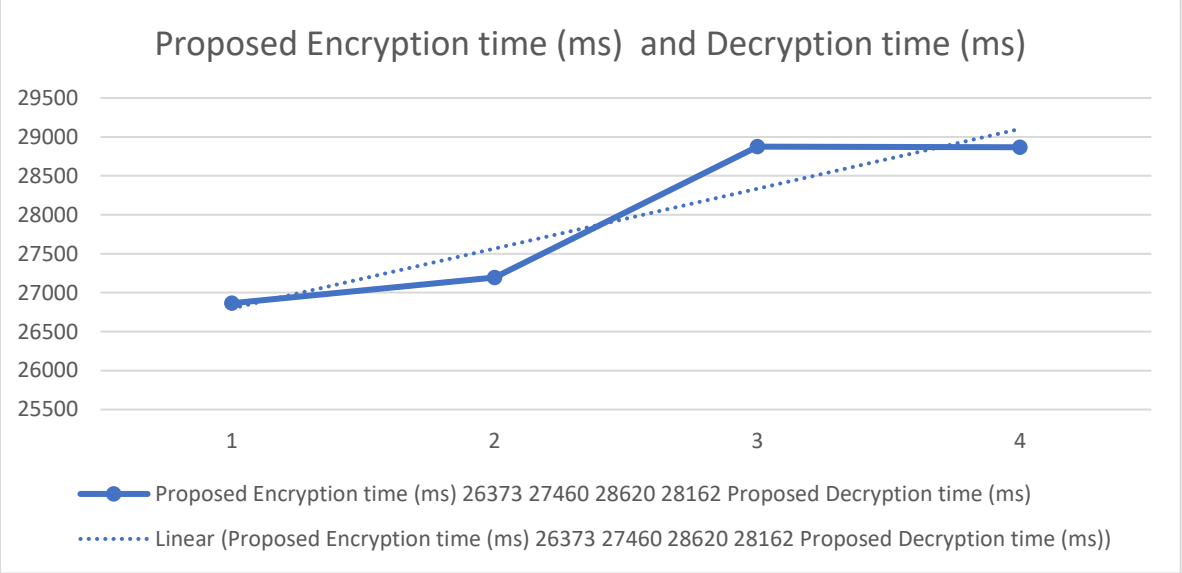

Figure 3: Proposed scheme encryption and decryption time graph

The proposed scheme time graph shows the geometric progression in both encryption and decryption time, we observed little decrease in encryption time between 28,620ms and 28,162ms. However, it does not affect the linear graph, 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.

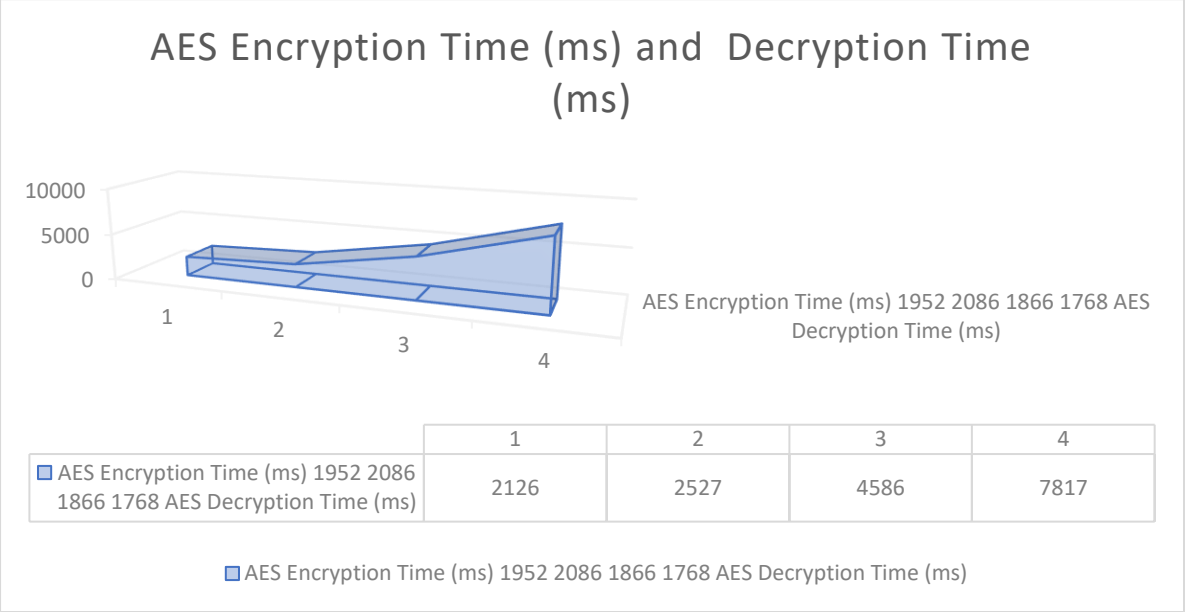

Figure 4: AES encryption and decryption time graph

We observed from figure 4 that decrypting an AES message using the same message size takes a longer time than encryption 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

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 for message sizes (m), both data_ experiments _2 and 1 produce ciphertext of the same size 157 bits, 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, which indicates 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 (Al-Aswad *et al.*, 2019) and (Hafid *et al.*, 2019).

REFERENCES

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

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

Su, Z., Hui, Y., Yang, Q. (2017). The next generation vehicular networks: A content-centric framework, IEEE Wireless Communications, vol. 24, no. 1, pp. 60–66.

Yang, Q., Zhu, B., Wu, S. (2016). An architecture of cloud-assisted information dissemination in vehicular networks, IEEE Access, vol. 4, pp. 2764–2770.
Huang, X., Yu, R., Kang, J., He, Y., Zhang, Y. (2017). Exploring mobile edge computing for 5g-enabled software defined vehicular networks, IEEE Wireless Communications, vol. 24, no. 6, pp. 55–63.

Firdaus, M., Rhee, K.H. (2020). 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.

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 Trans. Intell. Transp. Syst. 2018, 19, 2204–2220.

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

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

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

Hashemi, S.H., Faghri, F., Rausch, P., Campbell, R.H. (2016). World of empowered iot users. In IEEE 1st International Conference on Internetof-Things Design and Implementation, pages 13–24.
Xia, Q., Sifah, E., Smahi, A., Amofa,S., Zhang. X. (2017). Bbds: Blockchain based data sharing for electronic medical records in cloud environments. Information, 8(2):44.

Augot, D., Chabanne, H., Clemot,O., George, W. (2018). 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.

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

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

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

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.

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

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

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.

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.

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

Jiawen, Kang., Rong, Yu., Xumin, Huang., Maoqiang, Wu., Sabita, Maharjan., Shengli, Xie., Yan, Zhang. (2019). Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks, in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019, doi: 10.1109/JIOT.2018.2875542.

Muhammad, Arif., Guojun, Wang., Md Zakirul Alam, Bhuiyan., Tian, Wang., Jianer, Chen (2019). A survey on security attacks in VANETs: Communication, applications and challenges, Vehicular Communications, Volume 19, 100179, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2019.100179.