JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO 3

Implementation of VANET Security using SHA3-256 for Blockchain with Digital Signature in Python

Liqaa Saadi Mezher[1,2], Muna Hadi Saleh[1]

[1]University of Baghdad, College of Engineering, Electrical Engineering Department, Baghdad, Iraq
[2]Mustansiriyah University, College of Engineering, Computer Engineering Department, Baghdad, Iraq
E-mail: leqaa.saady2302p@coeng.uobaghdad.edu.iq, iqa35@uomustansiriyah.edu.iq, dr.muna.h@coeng.uobaghdad.edu.iq

Abstract

Vehicular ad hoc networks are quickly gaining popularity and are one of the most researched areas of wireless networks as they enable intelligent transportation systems that will provide various key services, including road safety, traffic management, and infotainment, with the goal of enhancing a driver's productivity and quality of life for all, either as commuters or as travelers. However, while these services offer significant benefits, they also require integration through robust and reliable communications of vehicles, which can only be achieved if security is properly taken into account. Public key infrastructure and cryptography previously implemented for controlling access are not a cost-efficient or scalable solution.
A new direction has been developed by the relevant norms, the blockchain. This is a public decentralized database based on Bitcoin. Blockchain consists of blocks in sequential order, in which calls of transactions are coupled in digital form to a hash function to form a chain. Then, calls in blocks are digitally signed to ensure that transaction integrity is maintained, and transaction contents are both checked and approved by the nodes. As regards applications for traffic ad hoc networks, smart contracts can offer an alternative path to increase system automation. In blockchain, there are several security areas, such as digital signature, integrity of the insecure distribution channel, and steganography, which is one of the main cryptographic techniques used to address VANET security problems. The main objective of this study is to evaluate VANET safety and how the security of blockchain is improved. Ad hoc network techniques and the SHA3-256 algorithm were developed to enhance security called Digital signature-based quantum secret key algorithm cryptograph and were used to improve blockchain security. The proposed approach can be useful for securing a more-safe system, including related security applications for vehicular ad hoc networks. The security discussed is not limited to VANET and blockchain, but also to ad hoc network communication vehicle to vehicle and vehicle to infrastructure. In addition, this poses a number of VANET challenges in a future direction.

Keywords: VANET Security, SHA3-256, Digital Signature, Blockchain, QSKA, Python.

1. Introduction

Vehicular Ad-hoc Networks (VANETs) are a subclass of Mobile Ad-hoc Networks (MANETs) that refer to the emerging major technology of wireless ad-hoc communication networks consisting of cooperative vehicles **Error! Reference source not found.**[1]. VANETs serve as the backbone of Intelligent Transportation Systems (ITSs), and their field of application is growing fast with the availability of technology

[3]. Wireless communication among vehicles or between a vehicle and roadside infrastructure has the potential to redefine the landscape of mobility safety, comfort, energy use, and reduction of environmental impacts [4].

The efficient operation of vehicular communication networks opens up enormous opportunities, but the lack of adequate security can lead to extremely serious societal and individual risks. Therefore, it is imperative to avoid or reduce such circumstances, e.g., a vehicle collision redirected by adjusting traffic signals or even remotely launching airbags **Error! Reference source not found.**. To overcome these hurdles, various research avenues need to be explored. Different technologies and techniques have already been proposed to address the security and privacy-related issues associated with VANETs. Among them, blockchain and digital signatures are considered potential solutions to enhance the security and privacy of VANETs.

The introduction begins with the relevance of VANETs with examples, creating the necessity to secure these networks. The introduction reflects on the relevance of technology in shaping the transportation sector. It outlines the risks due to insecure vehicular communications networks. Besides this, it gives an idea about the paper's intentions and objectives, taking a structured approach. Also, it presents four subsection headings.

1.1. Background and Motivation

VANETs are designed in the paradigm of Vehicle-to-Vehicle (V2V) as well as Vehicle-to-Infrastructure (V2I) technology for intelligent transportation systems (ITS) [5]. VANETs exhibit several potential benefits such as traffic information, collision warnings, emergency warning messages, lane changing, electronic payment of road tax, repudiation, overtakes, and environmental pollution reduction [7]. Despite this trend and in addition to the fact that VANETs contribute to numerous advancements, VANETs are more threatened by various security attacks compared to existing network environments. Indeed, it is quite essential to secure communication in VANETs to enhance network trustworthiness, make the network robust, and avoid casualties on the road. In the meantime, this latest technology needs other types of security equipment. Frequent message forwarding in multihop environments makes it easier for attackers to sit on a poorly monitored network **Error! Reference source not found.**.

Security solutions need immediate attention to enhance vehicle network security. Thus, it can be deduced from the existing case study that new security structures need to be included. Moreover, current security systems sometimes offer trivial services such as replay, DoS, and masquerade attacks, which are not sufficient to secure vehicle networks [8][9]. In vehicular communication, security plays an important role in different applications of the Internet of Vehicles (IoV). In VANETs, there are several security issues such as Sybil attacks, DoS attacks, and topology attacks. These attacks are handled using security mechanisms of blockchain, mainly used for secure communication. So, bringing both together would provide a better security solution for the VANET. Blockchain is used to identify the valid transactions that are to be accepted in the network, and a cryptographic technique is used to transfer the data into the form of a hash **Error! Reference source not found.**. The hash will be transferred over the

network, and then the digital signatures are used on the hash, which is encrypted with a quantum private key and decrypted with a quantum public key over the network. Hence, it is a good mechanism for the security of VANETs.

1.2. Research Objectives

The rapid development of technology has led to many threats that can be used by people with criminal intent. One such area is the damage caused by vehicle accidents. Road accidents have frequently occurred and have caused a high fatality rate [12]. There are several reasons for road accidents, one of the main ones being human error. Many researchers and car makers have been working to solve these problems by applying the concept to vehicles. However, the application of this technology brings new threats [13]. Currently, many security solutions have been proposed, but they help the system not yet reach the high security level due to the rapid development of information technology.

The main goal of the study is to improve the security of the system by using innovative integrated technology. From the research goal mentioned above, the following are the research objectives that will be achieved in this final paper. An important part of this paper is the goals that will be achieved as follows: 1) To develop a framework that is integrated for safely exchanging data between vehicles and roadside infrastructure. 2) Analyzing the results of a combination of technologies in securely exchanging data. The design of the research will be carried out according to the standard, which starts with the formulation of the problem and objectives, and then determines the methodology selected in this study. The methodology of this paper is a qualitative-quantitative approach. The resulting prototype model will be developed by using a python programming language.

2. Vehicle Ad-hoc Networks (VANET)

Vehicular ad hoc networks (VANETs) have become one of the most vital fields in road transportation [14]. VANET are a type of MANET used for real-time data distribution among vehicles. They have been widely applied in real-time fleet coordination, cooperative driving and dynamic routing **Error! Reference source not found.**. There are a number of potential attacks because of these challenges and risks. These attacks can be divided into several categories: confidentiality and message tampering, unauthorized access, traffic eavesdropping and surveillance, and a range of denial-of-service attacks [16]. The first three categories pose potential threats to traffic safety as well as personal privacy, while the last three jeopardize the overall system integrity. The VANET architecture is shown in the figure (1) [17].

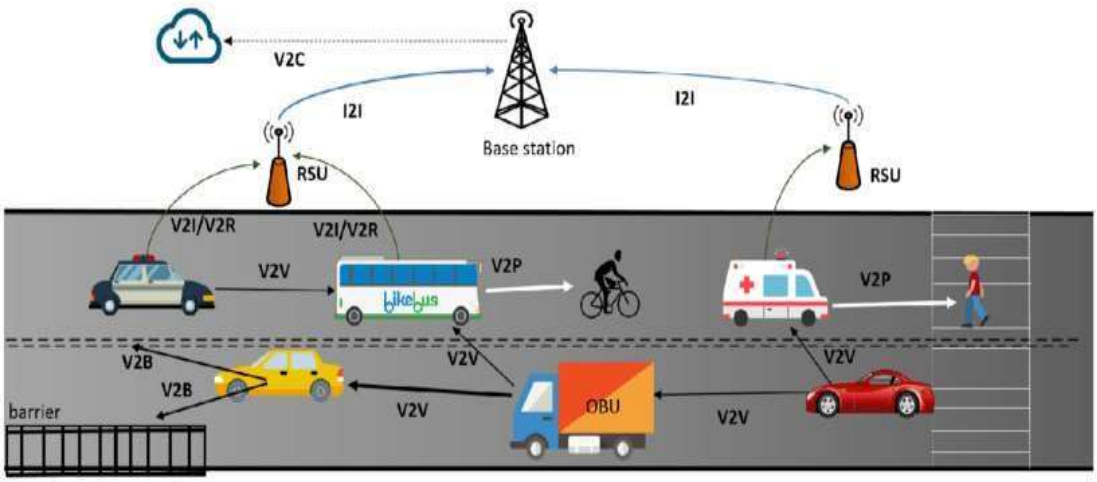

Figure (1) Architecture of VANET

In this architecture, vehicles utilize wireless transmission for information exchange. VANET has the following components: Roadside Infrastructure and Onboard Unit (OBU). The roadside infrastructure applications send and receive data to and from OBUs via RSUs, which are mounted at the roadside **Error! Reference source not found.**[18]. In order to enable vehicles to follow modern techniques for safety and cooperative driving, a radio box is built into the vehicle's electrical system. The OBU device can send and receive safety messages to and from neighboring vehicles and RSUs. In general, an architecture consists of three types of components [20].

The first one is the roadside infrastructure, which constitutes the roadside units (RSUs). The RSUs are placed at roadside locations and are connected to the RSUs for sending and receiving data to and from the vehicles that pass through the roads. In some VANET systems, RSUs are connected to the internet, so that RSUs can also send received data to the central server. The connectivity from RSUs to the central server is done with the help of the Internet Service Provider. The next and most important component is the Onboard Unit (OBU) of the vehicle in VANET. The OBU is placed inside the vehicle and acts as a client for vehicles. It receives messages from surrounding vehicles and performs the requested traffic sensing. The OBU performs sensing activities as it comprises various sensors. The sensors can include GPS, ultrasonic sensors, and carbon monoxide sensors **Error! Reference source not found.**. The communication in the VANET network can be done with intra-vehicle communication, where the communication occurs between vehicles (V2V), such as their current location, speed, and direction, and also with the roadside infrastructure, where the communication occurs between vehicles and the roadside infrastructure (V2I), The communication between the intra-vehicle and the roadside infrastructure follows some standard protocol [22][23].

3. Blockchain Technology in VANET

Decentralizing database management is the main principle and technology involved in a blockchain. Here, the term decentralizing is represented by a distributed ledger, complex cryptographic hash, and the coordination of the transactions [24]. A group of transactions is combined to form a new block; the hashing is processed on the created block, and the

resultant is called the block's hash value. The hash of the current block points to the previous blocks of data, making the entire chain secure and immutable. Blockchain amendments will not be made unless more than half of the network is involved in the process. Thus, the data in the blockchain is safe and transparent [25]. This feature allows for a higher degree of security in the system by removing single points of failure or control. The concept of transparency is another important characteristic of blockchain that enhances the security of the system. This feature offers a quick and easy way for any entity to verify the validity of the stored transactions.

Strings of data, which are usually represented as numbers, are hard to modify with the same constant hash. Each of the transactions is combined to form a new block, and to do this, an agreement is required between each node about the sequence of the transactions. The hashing is performed on the data in the block, and the resultant hash is stored in the block itself [26]. From time to time, the hash is created for every new block, and it also includes the hash value of every previous block in the network. This created pattern of hashed blocks is considered the blockchain, as shown in figure (2).

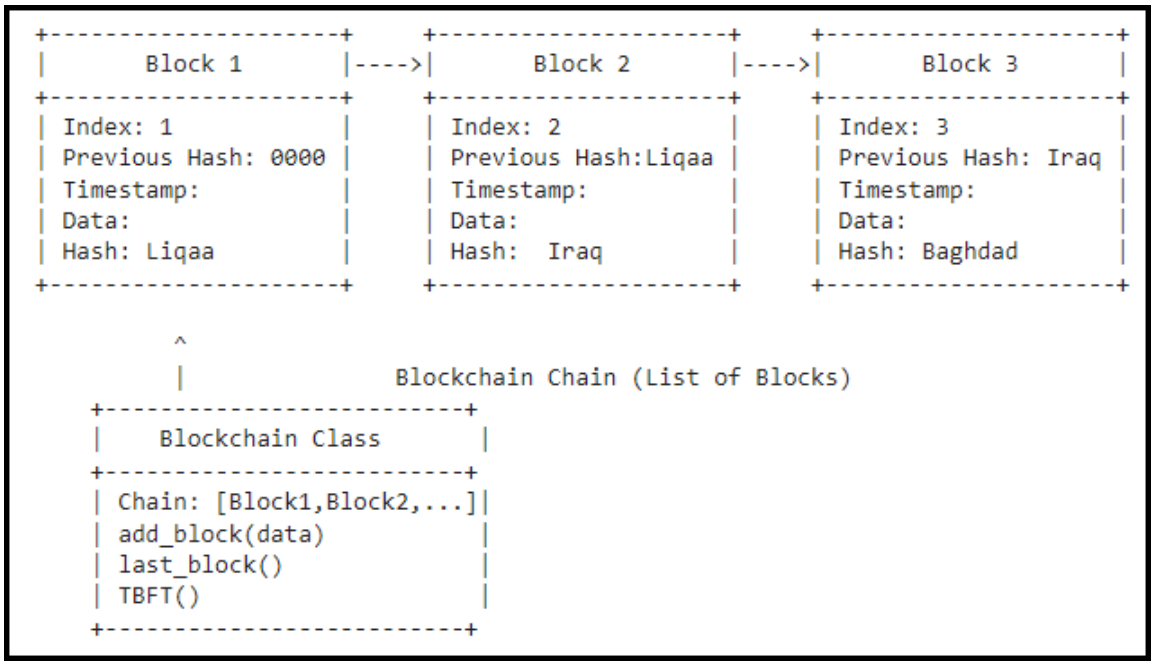

Figure (2) Architecture of Blockchain in Python

Blockchain is a distributed ledger, providing tools for coordination between independent nodes, exchange of data in a trustless manner, and giving finality of operations [27]. Blockchain is secure by design and is an example of a distributed computing system with high Byzantine fault tolerance. Blockchain was invented to serve as the public transaction ledger of a cryptocurrency [28]. The invention of the blockchain for this cryptocurrency made it the first digital currency to solve the double-spending problem without the need for a trusted authority or central server **Error! Reference source not found.**. To accomplish this, the blockchain is the most secure, and the built-in measures of the communication are used for the implementation of the communication process by the technology. In the context of VANET, details about the status of transactions

between various vehicles collected and stored on the blockchain network enhance the integrity and security of the VANET system.

4. SHA3-256 in VANET

4.4.1. SHA-3 Family of Secure Hash Algorithms

The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions that can compute a fixed-size digest of an input block or message. The SHA-3 family of hash functions was standardized to provide better security and performance compared to their predecessors, as shown in table (1) [29]. Among those, SHA-3-256 is functionally built on the Keccak-F algorithm designed to process 1600 bits. The structure of SHA-3 makes it drastically distinct from the SHA-2 family of algorithms, making it resilient to the same kinds of attacks. In particular, SHA-3-256 was designed with an extended security margin of 256 bits.

Table (1): Comparison of SHA-3 Parameters standard, (all sizes are measurement in bits)

characteristics	SHA3-224	SHA3-256	SHA3-384	SHA3-512
Message size	No maximum	No maximum	No maximum	No maximum
Block size (bit rate r)	1152	1088	832	567
Word size	64	64	64	64
Message Digest size	224	256	384	512
Number of rounds	24	24	24	24
Capacity (c)	448	512	768	1024
Collision Resistance	2^{112}	2^{128}	2^{192}	2^{256}
Second Preimage Resistance	2^{224}	2^{256}	2^{384}	2^{512}

4.4.2. SHA-3-256 Algorithm

SHA-3-256 has a block length and message digest size of 1600 bits and 256 bits, respectively [31]. The input message to SHA-3-256 goes through the padding scheme and is then recomposed into a 1600-bit array of fields, constituting the internal state of the algorithm. The internal state is transformed using the permutation-based operations (rounds), producing a 256-bit hash value. SHA-3-256 is resistant against three types of attacks in cryptographic algorithms [32]. Even if another input value would result in the same output hash value, as shown in figure (3), it must take an indeterminable long time to find such an input. Resistance guarantees that it is impossible to ascertain an input from its hash value, and that an existing input would not produce the same hash when hashed. The SHA-3-256 algorithm can therefore be applied for secure digital signatures, proof of ownership, message authentication codes, and blockchain transactions.

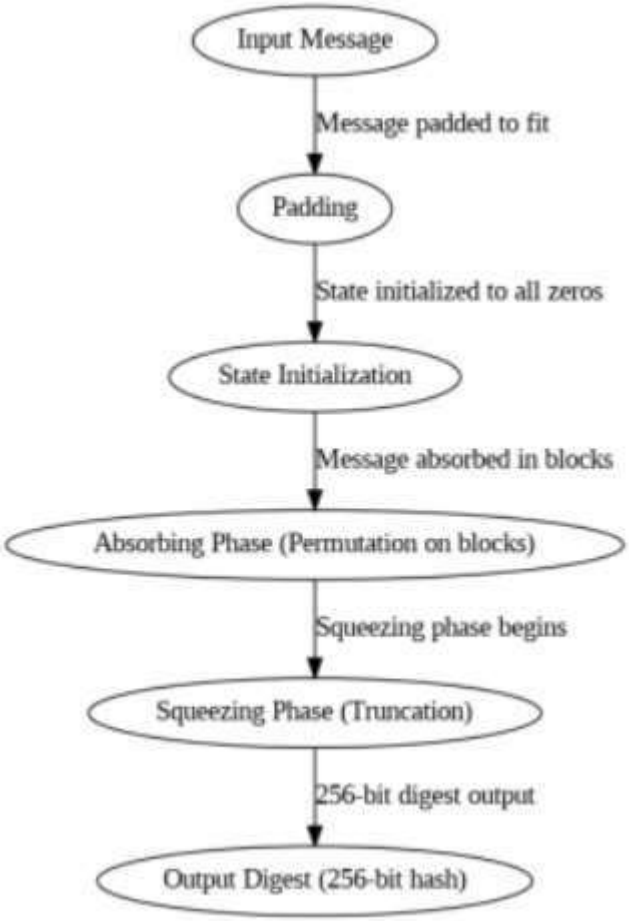

Figure (3) Flow Char of SHA3-256 Algorithm in Python

5. Digital signature in VANET

Definition A digital signature is a process whereby a document, package, or any kind of data sent over VANET is signed by a known entity in a distinctive way that the signature cannot be duplicated, forged, or contradicted by anyone else but the originator [33][34]. It is based on cryptographic techniques using secret keys. Each such creation consequently needs to be unique and particular to that transaction. It offers a high level of assurance on the following features: - Data Integrity - Authenticity - Non-Repudiation In today's digital world, with respect to data communication, the digital signature is a critical factor for business and government and can be used between citizens [35].
A digital signature is a mathematical technique that ensures the authenticity and integrity of the data because it verifies the sender's identity [36]. A digital signature is the same as a written signature in a printed document. It is used to verify and authenticate the signer of the document or data. A digital signature can be used with every kind of message, whether it is encrypted or unencrypted. A digital signature uses techniques of cryptography such as quantum public key cryptosystems to create a key pair. The first key is quantum public and the second key is quantum private. When the data, like a message or document, is encrypted with a quantum private key, then this signature can

be verified by the receiver with the help of the sender's quantum public key [37]. If the quantum public key is valid for the signature and it is verified, it means that both the integrity and authenticity are preserved.

If a message or document has a signature and declares that it is signed by sender, in this situation, if the receiver uses the quantum public key of sender and it is verified for the message, then the sender, will not refuse that this is a false signature. He can't repudiate the message because this is written and signed by him. This can be beneficial for the receiver because it has a digital signature [38]. Likewise, if any message or document is signed by someone else, then sender has to sign a message because he has to agree with the signature. Before it is going to be verified, it is signed by sender. After installing the receiver's machine, the quantum private key is installed in the sender's machine. A digital signature is created with a pair of different hash functions [39]. Digital signatures are used in message protocols, certificates, and authentication. Digital signature technology has placed in a cryptographic key pair that consists of a quantum private key and a quantum public key. The quantum private key is used to create the signature, and the quantum public key is used to verify the signature. The digital signature uses a pair of cryptographic hash functions. Digital signatures verify the information or data of the sender. Some practical applications of digital signatures are in secure messages, software distribution, copyright, e-voting, contracts, cheques, and other forms of electronic documents. It is also used in some security protocols. Highlighted is secure connection, which can be viewed as a vehicular ad-hoc network using wireless technology to communicate securely. Moreover, the inter-vehicle communication and in-vehicle communication are secured with digital signatures, and wireless communication over a mobile network secure connection is done using a digital signature [40]. It should also be noted that standards are in place for digital signatures, supporting secure communication and validated use as of now. However, there are some known security-related issues related to proposed applications that could be addressed with security techniques such as QSKA, as shown in figure (4).

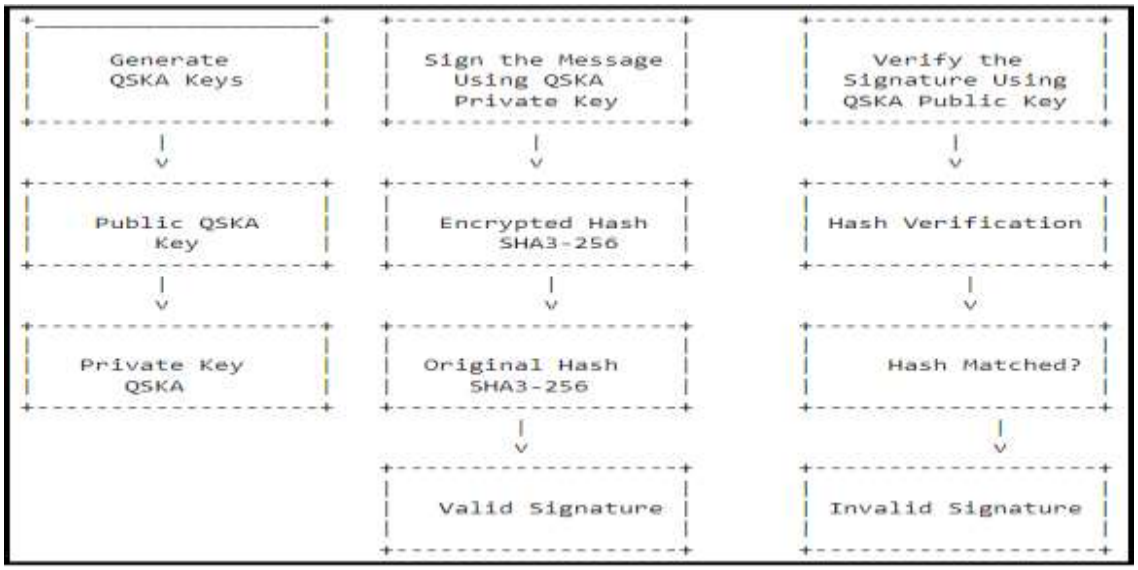

Figure (4) Architecture of Digital Signature in Python

6. Quantum Security Key Algorithm (QSKA)

QSKA is performed iteratively in two stages. Initialization Stage: kSKQA

1) Selection of quantum qubits (2n + 1) in a specific sequence.
2) Assign original data and auxiliary information symbols of n block binary symmetric key by amplitude using the Hadamard matrix [41].
3) Then apply the Kronecker product with as many quantum qubits as possible to create a composite symmetric key mask [42].
4) Repeat the Kronecker product of the quantum qubit mask with the quantum qubit mask for every two qubits as per the basic composite symmetric mask rule **Error! Reference source not found.**.
5) After applying the quantum Kronecker product with q1q2, the new composite symmetric key undergoes a permutation stage by shuffle [42].
6) As of now, the output of the population is a randomly generated key through permutation of shuffle and Kronecker product operation.
7) Now, for easy selection of kSKQA, apply reduction of the composite symmetric key using quantum inverse transformation.
8) In reverse order, compute the specific sequence matrix of Hadamard by using inverse transformation, and then each amplitude is fetched based on the shuffled order matrix that is omitted. Parallel Computation and Conditional Probability Change [41].
9) The probability or key frame obtained is easy if many multi-core chips provide sufficient permutation jobs. With more processing power, it works quickly to achieve results immediately. In this stage, the bit sequence is selected, and the condition is tested one by one with the block bit frames. The condition means that the sequence of key value bits is similar to its surroundings or not.
10) The testing of addressing is employed 255 times on the original bit. At first, the gradient is always an even number utilizing prime. After that, three more qubits are tested for prime bits and divided by the specific block of block size n^2.
11) If the binary compared value encounters another same value, it will be displayed, and similarly, another two same values are also displayed. The shadow of prime communication is done in that particular block. The threshold of prime is incremented cyclically day by day after every comparison.

7. Related Work

Vehicular Ad Hoc Networks (VANETs) are designed for seamless vehicle-to-vehicle and vehicle-to-roadside communication. There is much security-related research and development to enhance VANETs' security systems. Our study outlines the current research and advancements available for improving secure VANETs. The findings are systematically categorized into cryptographic techniques, consensus mechanisms, and protocol designs based on the approach according to the establishment of the system. In the current literature, the comparative analysis of different approaches found that there are no broad techniques in VANET to resolve automotive security problems. It is difficult to single out an approach that is more appropriate than the others relative to the design and enhancement of security. Our study proposes to design a new cryptographic algorithm that can facilitate new services. However, these papers are insufficient to

demonstrate the implementation of SHA-3-256, blockchain, and digital signatures in the VANET protocol.

The study proposed in this paper establishes the connection with several findings of research papers that do not address or have limitations in proposing a new system, such as implementing secure communication in integration with intrusion detection. Using the quantum key distribution system as an enrichment for secure communication is the emphasis of the comparison of the design proposed. Overall, the literature review revealed that there is no work in the proposed system that addresses or integrates blockchain design with secure VANET systems as a secure communication transmission enhancement. Therefore, this paper introduces a robustness-encryption technique using the SHA-3-256 algorithm to strengthen the digital signature and integrate it with blockchain technology to enhance the VANET network's reliability.

8. Implementation in Python

Python is a general-purpose programming language used for the implementation of the proposed framework [44]. To implement security for VANET, each vehicle in the network must compute the incoming packet and check if it fits a set of predefined rules. After a vehicle has verified and validated the received packet, a legitimate vehicle will broadcast the block to notify all neighboring vehicles [45]. The block is forged using the SHA3-256 algorithm to hash part of the incoming packet. Then, the hash value is computed with the SHA3-256 algorithm [46]. Blockchain and digital signatures are used to ensure the reliability of the transmission. V2V is used so that vehicles move from one place to another as in the real world. Vehicles can communicate with other vehicles in their neighborhood. Finally, we discover that communication in a collaborative community is the key to making off-route hacking expensive, rendering incentives unprofitable, elusive, or both. This work focuses on the feasibility of security and the distributed ledger of a blockchain-controlled security VANET through SHA3-256 by adopting some previous work in simulation. Evaluation of the experiments is presented by using a Python program for the SHA3-256 example. Python provides an easy-to-use and efficient platform for practitioners to adopt the concept and implement the proposed framework in vehicle to achieve the distributed ledger of the blockchain to ensure the security of VANET in the current IoT technology. This will inspire the research community for further research. The key innovation of the paper is the concept of using SHA3-256 and digital signature for blockchain in VANET by using QSKA.

9. Integration of Blockchain and Digital Signature in Python

Blockchain technologies can effectively be integrated with cryptographic mechanisms and various modern tools to provide secure data transactions [47]. The digital signature, which works on the concept of quantum public key cryptography, can be integrated with the blockchain to enhance overall security against attacks [48]. In this paper, blockchain technologies can be effectively combined with the main idea of digital signatures to secure the VANETs. The combined work was carried out in Python. Here, the SHA-256 cryptographic hash function libraries, serialization libraries, blockchain libraries and cryptographic libraries of Python were used.

Used combining blockchain technology with the concept of a digital signature, achieved security against external threats. The data stored in the blockchain is hashed with a cryptographic hash function that will give a unique data signature, and we used elliptic digital signature functions for more security, as shown in figure (5). Finally, the sent vehicle will update its block with the propagated block to its blockchain based on the longest chain rule. The cryptographic digital signature also updates the list used to control the misbehaving vehicle being allowed to propagate the wrong data. To achieve and implement that, integrated the above-discussed concept in Python. Developed this concept by simply using Python. Initially, installed the necessary libraries and then wrote the specific code that [49]. Then, divided our implementation phase into input, processing, and output. We must overcome the limitations of the existing systems, such as latency and data handling for different conditions. The environment of these systems is critical to ensure realistic performance, evaluation, and analysis.

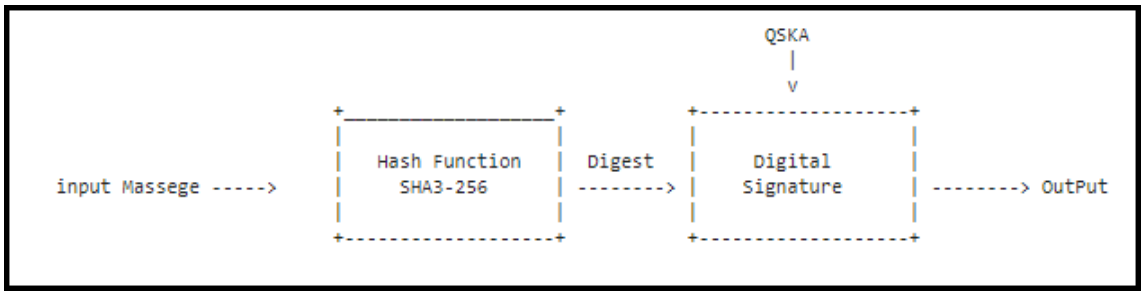

Figure (5) Block Diagram Blockchain with Digital Signature in Python

10. Case Study

In this paper, used the number of vehicle (10), and security hash function with round 3 and fixed length of output (256 bits) is called digest, this output will be input as a digital signature with the QSKA to extract the encrypted message to increase the safety, as shown in table (2).

QSKA = b'KYEw923F2jjloqAt93Tj0zyjxBmvbllntnSgkxDXGLo='

Table (2): Encryption the Message by SHA3-256 with Digital Signature

Number of Block	Message	SHA3-256	Digital Signature
0	Message from vehicle 1	85e76824f887a05657cf642 8b2a43b0d2f58b7d2f3217b	a1a92904514677e8549ffef70 422b419216007d416ac77
1	Message from vehicle 2	73a76d7fab9b6cc971eaa54 6ac1e25f1690039137fac1e	2f96e944bd9322137d4cdec26 cc4a88c59cc41df5614f9
2	Message from vehicle 3	88717ddbd366e3012d0319 6e358dc6bf9325f47155d43	489d184e4141b8730fb1aabc9 04a9f14141f67949a8686
3	Message from vehicle 4	7744b4c786e9323dac7bbfd 91ce835c56f3090fea77e02	4d6d30d5dc0e02a4254a8c2f1 dee48f42bbe8625cd71d8
4	Message from vehicle 5	899e92fef242b8c7365eee3 e7392cc7f224d144057bbbe	8a3ee48ddc0a97bae121cffd9e ceb6b6938d89b5cb223e
5	Message from vehicle 6	07425efea0d5572fd720de1 b0a55134e7dea2773d796ed	550df71b61152129c62d9b49 d3a9bd82c5a7a26125e841

6	Message from vehicle 7	4de6e08dceed78dcbfa3297 64d7ca4de5c18ad36cd8eba	32b7af2ad4fe7eea98c79102b dc20e1a3aa0acc87d6da2
7	Message from vehicle 8	9fe8d194893fe08a56cb6e5 64a1efbeee0005be99cea65	643a561ac4fac9d317cbe97ff0 576d8e3cda3a80d2d1ed
8	Message from vehicle 9	3004ef2aad3fedd3a32edcaf 2b9f0fc131a6af81eb2868	39a5735c16be2ea3ea8f947a2 90c86889fb9d6923c2785
9	Message from vehicle 10	72e214c18ac69f50d536fb9 15c63363047fadb7e0d272d	7fe4e1cc858851e2f77326f1d3 68d23dd2332d929cb75a

11. Results of integrated SHA3-256 for Blockchain with digital signature using QSKA

In the paper, integrated SHA3-256 for blockchain with the digital signature in Python and tested the program using a truthful attacking case. The goal for this case is to demonstrate that, by using SHA3-256 for the blockchain, a fake vehicle cannot change its data in order to benefit from that change to the route instead of a truthfully attacking vehicle. The metrics to measure are a truthful attacking vehicle, a fake vehicle, and a truthful blockchain. A truthful attacking vehicle sends and receives messages truthfully, whereas the values of messages from a dishonest vehicle are different from the truth. A truthful blockchain stores messages in order using hashing.

This section presents the experimental study and analyzes the results. The security system was tested using several measures. These measures include successful and failed attacks, key usage time to check how frequently the users receive safety messages, and time taken, which includes the process of signature verification using different lengths of keys in the blockchain.

observed the ability to detect attackers and the effectiveness of theft prevention through the attacker's manipulation within the integrity of data in vehicular ad hoc networks. In networking, keys are used to minimize the presence of data theft and ensure authentication. The system has installed part of the blockchain onto cars and has shown how a blockchain can prevent this attack in the real world while the channels are using its location. Confirm whether blockchain technologies are worthy of interest and can serve VANET security. The results from the analyses using RSA with QSKA symmetric and asymmetric show significant. This analyzes how well blocking off attackers can prevent theft in the confidentiality of data provided. This verifies through the non-tampered integrity of chained blocks after being stolen. Generally, the system could detect attackers and not reveal the identity of the engines while comparing the evaluation of different techniques. The study has strengths in terms of promoting the future development of blockchain security systems working together with digital signatures for vehicular networks. With security systems like this, it could lead to the characteristics of confidentiality and integrity. Furthermore, it can detect fake requesters, and there is no feature revealing legitimate receivers.

As for the honest case, vehicle 1 reads message 1 from the last car with SHA3-256 and concatenates the result into message 2 along with extra data: message 2 = (SHA3(message 1) || extra data 2). Vehicle 1 forwards message 2 and keeps the quantum private key for its quantum public key to sign message 2. The leader reads message 2 with the digital signature using SHA3-256. Vehicle 1 also sends back the extra data as a separate message, message 3, to all vehicles behind the leader; extra data 3 = extra data 2, to finish that same vehicle can read the following message and attach its quantum

private key that corresponds to its quantum public key to sign the information. Vehicle 1 has to update message 3, a driving-assistance message, at high speed as soon as possible to avoid a vehicle crash. Any risk of a vehicle crash by following inaccurate instructions neglects cost-effectiveness and increases the computing processing time for a crash warning, as shown in figure (6).

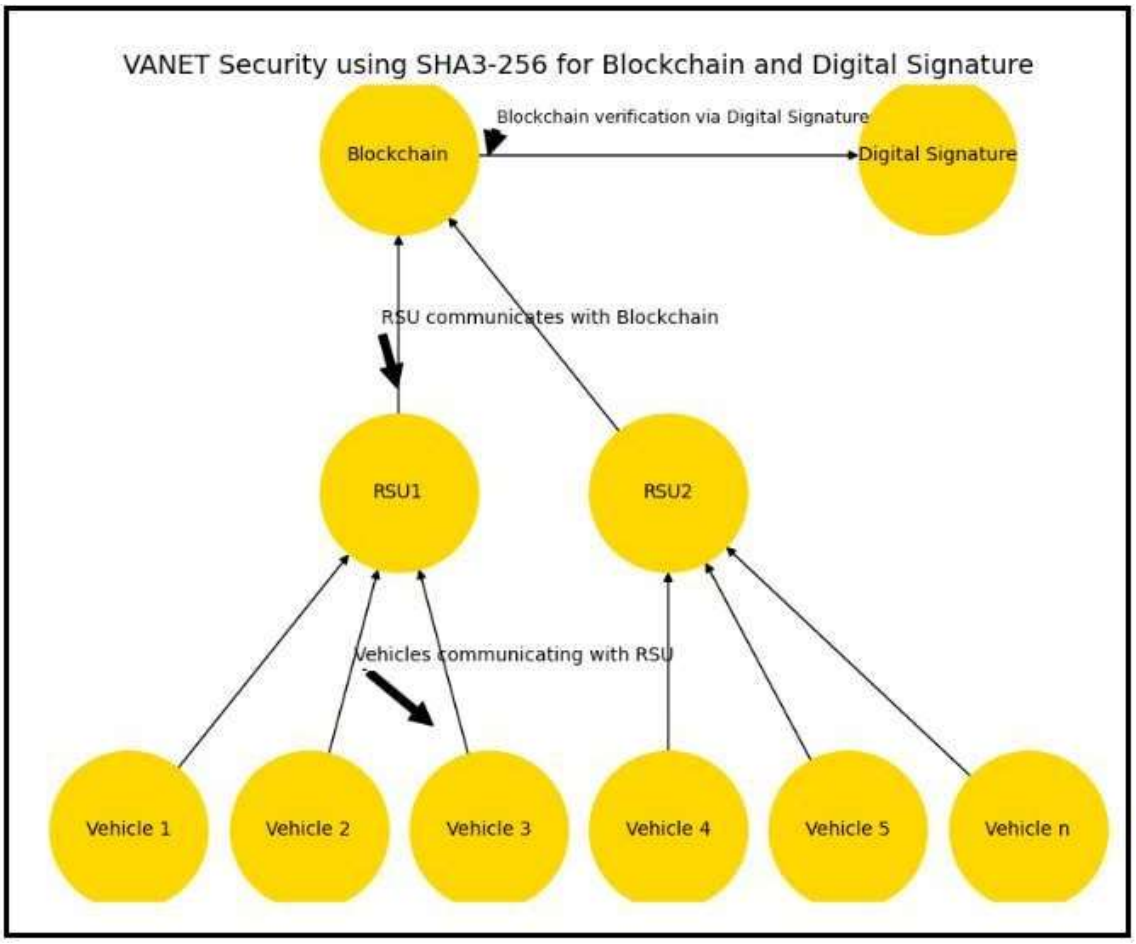

Figure (6) Integrated SHA3-256 for Blockchain with Digital Signature in Python

12. Conclusion and Future Work

A . Conclusions

In this paper, suggested a new secure vehicular ad hoc network architecture by combining three methodologies: connection SHA3-256, blockchain technology, and quantum secure key agreement with digital signature. Also, presented a new symmetric and asymmetric key quantum scheme based on multiple quantum qubits using the Hadamard matrix for the enhancement of security keys. The application of Hadamard matrix formation for the composite symmetric and asymmetric key qubit provides quick and strong masking for the delivered key, making it easier to merge combinations of information bits. The reuse of bit positions of the transformation bits is effectively fulfilled to the required order. The performance comparison of NIST and QSKA driving characteristic implementation proved that superior results were provided by digital

signature, with a reduced success rate for possible eavesdroppers and modified schemes. This way, an eavesdropper is unable to get the connection keys. The encrypted connection quantum key is then posted in the system, and the claimant needs access to a valid blockchain to get the key to establish the connection with the access node. Finally, this claimant is able to get the connection key using the quantum key to establish the link with the access node that had sent the connection key using the same quantum key in a secure and secret way. The proposed architecture is implemented, and the results display the working principle and concept with no logical errors, as expected.

B. Future Work

This work considers the security issues that researchers aim to protect through the technologies currently available and is worth deploying. However, due to the dynamic nature of technologies, present or emerging new technology might enhance the features of vehicular network security in the future. Hence, the security measures in the VANET systems can be further adapted for the following new technologies: (1) without using a communication infrastructure to facilitate inter-vehicle communication, vehicular communication can be performed using emerging technologies; (2) emerging technologies such as data mining algorithms could be implemented to increase the security of data in vehicular communication; (3) an energy-efficient, dynamic, and delay-sensitive intrusion detection system can be developed that combines gossip data diffusion for detection with blacklisting for reaction. These methodologies can be implemented on a real vehicle. Besides, faults can be inserted into the activation system to test the resistance and gain insight into how long this system may remain secure.

13. References

[1]. Ramamoorthy, R., & Thangavelu, M. (2022). An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3837-3868.

[2]. Alharthi, A., Ni, Q., Jiang, R., & Khan, M. A. (2022, June). A formal method of trust computation in VANET: A spatial, temporal and behavioral approach. In *International Conference on Smart Technologies in Urban Engineering* (pp. 775-784). Cham: Springer International Publishing.

[3]. Wang, J., Chen, Y., Ji, X., Dong, Z., Gao, M., & Lai, C. S. (2023). Vehicle-mounted adaptive traffic sign detector for small-sized signs in multiple working conditions. *IEEE Transactions on Intelligent Transportation Systems*.

[4]. Batool, H., Anjum, A., Khan, A., Izzo, S., Mazzocca, C., & Jeon, G. (2024). A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. *Information Sciences*, *652*, 119717.

[5]. Rashid, A., Al-karkhi, A. A. S., & Hassan, N. F. (2023). Wallet Key Generation for a Generic Blockchain based on Speech. *Iraqi Journal of Science*, 1487-1497.

[6]. Sanguesa, J. A., Barrachina, J., Fogue, M., Garrido, P., Martinez, F. J., Cano, J. C., ... & Manzoni, P. (2015). Sensing traffic density combining V2V and V2I wireless communications. *Sensors*, *15*(12), 31794-31810.

[7]. Padiya, P., Vidhate, A., & Vasappanavara, R. (2023). Cluster-based combined hybrid relay vehicle selection approach for improving performance and reliability in vehicular ad hoc networks. *International Journal of Communication Networks and Distributed Systems*, *29*(5), 532-554.

[8]. Mohammed, M. S., Abduljabar, A. M., Faisal, M. M., Mahmmod, B. M., Abdulhussain, S. H., Khan, W., ... & Hussain, A. (2023). Low-cost autonomous car level 2: Design and implementation for conventional vehicles. *Results in Engineering*, *17*, 100969.

[9]. Abdul-Jabbar, M. D., & Aldeen, Y. A. A. S. (2023). State-of-the-art in data integrity and privacy-preserving in cloud computing. *Journal of Engineering*, *29*(01), 42-60.

[10]. Vamshi Krishna, K., & Ganesh Reddy, K. (2023). Classification of distributed denial of service attacks in VANET: a survey. *Wireless Personal Communications*, *132*(2), 933-964.

[11]. Saish, N. V. P., Vijayashree, J., & Jayashree, J. Application of Blockchain in Medical Industry. In *Blockchain for Healthcare 4.0* (pp. 26-47). CRC Press.

[12]. IM Almadi, A., Al Mamlook, R. E., Ullah, I., Alshboul, O., Bandara, N., & Shehadeh, A. (2023). Vehicle collisions analysis on highways based on multi-user driving simulator and multinomial logistic regression model on US highways in Michigan. *International journal of crashworthiness*, *28*(6), 770-785.

[13]. Verma, U., & Sohani, M. (2024). An efficient lightweight authentication scheme for dew-assisted IoT networks. *Security and Privacy*, *7*(2), e360.

[14]. Maram, R. K., Ponnapalli, V. S., & Maddiboyina, H. V. (2021, December). Smart transportation and evolutionary algorithms: an approach to understand vehicular Ad-Hoc network. In *International Conference on Artificial Intelligence and Data Science* (pp. 476-489). Cham: Springer Nature Switzerland.

[15]. Zhang, J., Ge, J., Li, S., Li, S., & Li, L. (2023). A bi-level network-wide cooperative driving approach including deep reinforcement learning-based routing. *IEEE Transactions on Intelligent Vehicles*.

[16]. Chen, L., Zhu, J., Yang, Y., & Boichenko, S. (2024). Physical Layer Security for RIS-V2V Networks with Different Eavesdropper Locations. *IEEE Internet of Things Journal*.

[17]. Tandon, R., Verma, A., & Gupta, P. K. (2024). D-BLAC: A dual blockchain-based decentralized architecture for authentication and communication in VANET. *Expert Systems with Applications*, *237*, 121461.

[18]. Jasim, A. H., & Kashmar, A. H. (2023). An Evaluation of RSA and a Modified SHA-3 for a New Design of Blockchain Technology. In *Artificial Intelligence for Smart Healthcare* (pp. 477-489). Cham: Springer International Publishing.

[19]. Dias, D., Luís, M., Rito, P., & Sargento, S. (2024). A Software Defined Vehicular Network using Cooperative Intelligent Transport System Messages. *IEEE Access*.

[20]. Dutta, A., Samaniego Campoverde, L. M., Tropea, M., & De Rango, F. (2024). A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications. *Journal of Network and Systems Management*, *32*(4), 73.

[21]. Abhishek, L., & Kathirvelan, J. (2021, November). Design and development of IoT enabled gas sensing system for remote monitoring of air quality in borewell rescue operations. In *Journal of Physics: Conference Series* (Vol. 2115, No. 1, p. 012012). IOP Publishing.

[22]. Mohammed, D., Mansor, M., & Hock, G. C. (2024). Evaluation of the performance of the vehicular ad hoc network protocols in the case of V2I and EV2I communications. *Bulletin of Electrical Engineering and Informatics*, *13*(1), 222-232.

[23]. Qazi, F., Khan, S. A., Hanif, F., & Agha, D. E. S. (2024). Efficient Routing Algorithm Towards the Security of Vehicular Ad-Hoc Network and Its Applications. *International Journal of Wireless Information Networks*, *31*(1), 12-28.

[24]. Samadhiya, A., Kumar, A., Agrawal, R., Kazancoglu, Y., & Agrawal, R. (2023, January). Reinventing reverse logistics through blockchain technology: a comprehensive review and future research propositions. In *Supply chain forum: An international journal* (Vol. 24, No. 1, pp. 81-102). Taylor & Francis.

[25]. Yessenbayev, O., Nguyen, D. C. D., Jeong, T., Kang, K. J., Kim, H. R., Ko, J., ... & Comuzzi, M. (2024). Combining blockchain and IoT for safe and transparent nuclear waste management: A prototype implementation. *Journal of Industrial Information Integration*, *39*, 100596.

[26]. Shrivastava, P., Alam, B., & Alam, M. (2024). A hybrid lightweight blockchain based encryption scheme for security enhancement in cloud computing. *Multimedia Tools and Applications*, *83*(1), 2683-2702.

[27]. Albulayhi, A. S., & Alsukayti, I. S. (2023). A blockchain-centric IoT architecture for effective smart contract-based management of IoT data communications. *Electronics*, *12*(12), 2564.

[28]. Al-karkhi, A. A. S., Hassan, N. F., & Azeez, R. A. (2023). A Secure Private Key Recovery Based on DNA Bio-Cryptography for Blockchain. *Iraqi Journal of Science*, 958-972.
[29]. Falih, R. A., Jusoh, Y. Y. B., & Khadhim, D. J. (2023). New Research Trends in Designing E-Government Architecture Based on Blockchain Technology. *Journal of Engineering*, *29*(11), 17-36.
[30]. Jasim, A. H., Hammood, D. A., & Al-Askery, A. (2023, October). Design and Implementation of AES-SHA Security Hardware using FPGA. In *2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)* (pp. 1-8). IEEE.
[31]. Kim, D. S., Lee, S. H., & Shin, K. W. (2019, January). A hardware implementation of sha3 hash processor using cortex-m0. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)* (pp. 1-4). IEEE.
[32]. Bindu, G., Moyeenudin, H. M., & Anandan, R. (2023). Blockchain of Cryptocurrency Using a Proof-of-Work-Based Consensus Algorithm with an SHA-256 Hash Algorithm to Make Secure Payments. In *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations* (pp. 243-252). Cham: Springer International Publishing.
[33]. Wali, A., Ravichandran, H., & Das, S. (2024). A 2D cryptographic hash function incorporating homomorphic encryption for secure digital signatures. *Advanced Materials*, 2400661.
[34]. Chapman, J. C., Alshowkan, M., Qi, B., & Peters, N. A. (2024). Entanglement-based quantum digital signatures over a deployed campus network. *Optics Express*, *32*(5), 7521-7539.
[35]. Fang, Q. (2024). Designing of music copyright protection system based on deep belief network and blockchain. *Soft Computing*, *28*(2), 1669-1684.
[36]. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing. *IEEE Access*.
[37]. Rewal, P., Singh, M., Mishra, D., Pursharthi, K., & Mishra, A. (2023). Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices. *Journal of Information Security and Applications*, *75*, 103505.
[38]. Mohammed, Z. A., Gheni, H. Q., Hussein, Z. J., & Al-Qurabat, A. K. M. (2024). Advancing cloud image security via AES algorithm enhancement techniques. *Engineering, Technology & Applied Science Research*, *14*(1), 12694-12701.
[39]. Badawy, M. (2023). Security Evaluation of Different Hashing Functions with RSA for Digital Signature. *IJCI. International Journal of Computers and Information*, *10*(2), 99-116.
[40]. Durech, J., Franekova, M., Holecko, P., & Bubenikova, E. (2016). Modelling of security principles within car-to-car communications in modern cooperative intelligent transportation systems. *Advances in electrical and electronic engineering*, *14*(1), 49-58.
[41]. Xia, T., Zuo, G., Lou, L., & Xia, M. (2024). Hadamard matrices of composite orders. *Transactions on Combinatorics*, *13*(1), 31-40.
[42]. Chu, M. T., & Lin, M. M. (2022). A complex-valued gradient flow for the entangled bipartite low rank approximation. *Computer Physics Communications*, *271*, 108185.
[43]. Takeuchi, N., Yamae, T., Yamashita, T., Yamamoto, T., & Yoshikawa, N. (2023). Scalable quantum-bit controller using adiabatic superconductor logic. *arXiv preprint arXiv:2310.06544*.
[44]. Kim, M., Kim, P., Bassiri, R., Prasai, K., Fejer, M. M., & Lee, K. H. (2024). ePDFpy: A Python-based interactive GUI tool for electron pair distribution function analysis of amorphous materials. *Computer Physics Communications*, *299*, 109137.
[45]. Hong, J., Liang, F., Yang, H., Zhang, C., Zhang, X., Zhang, H., ... & Yang, J. (2024). Multi-forword-step state of charge prediction for real-world electric vehicles battery systems using a novel LSTM-GRU hybrid neural network. *eTransportation*, *20*, 100322.
[46]. Chenchev, I. (2023, February). Speedup of Merkle-Root Hash Value Computation Using Groups. In *Future of Information and Communication Conference* (pp. 259-280). Cham: Springer Nature Switzerland.
[47]. Kumar, B. A., & Bapuji, V. (2024). Efficient privacy preserving communication protocol for IOT applications. *Brazilian Journal of Development*, *10*(1), 402-419.
[48]. Dhinakaran, D., Selvaraj, D., Dharini, N., Raja, S. E., & Priya, C. (2024). Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution. *arXiv preprint arXiv:2407.18923*.
[49]. Maitin, A. M., Nogales, A., Chazarra, P., & García-Tejedor, Á. J. (2023). EEGraph: An open-source Python library for modeling electroencephalograms using graphs. *Neurocomputing*, *519*, 127-134.

Muna Hadi Saleh received a B.Sc. in Control and Systems Engineering from the University of Technology (1988-1989), she received an M.Sc. in Control and Instrumentation Engineering from the University of Technology (1995-1996) while her Ph.D. in Computer and Information Technology from University of Technology (2005 2006). Now she is a Faculty Member of the Electrical Engineering Department of Engineering-Baghdad University. She published Forty-four papers and supervised M.Sc. and Ph.D. students. Finally, she is aresearcher in many conferences, and she has scientific experience in IEEE, and JESTEC, also she is a member of IAO. Her field of interest and her research works focus on AI, Intelligent Methodology, Soft Computing, Neural Networks, Fuzzy Logic, Genetic Algorithm, Automation Control, Robotics, Computer Architecture, E-Learning, Data Mining, Rough Set, Wireless Sensors, Deep Learning, Machine Learning, IoT, Modern & Classical Control, Flight Control, UAV Control, Classification Data set methods with cloud Computing. She can be contacted at email: dr.muna.h@coeng.uobaghdad.edu.iq.

Liqaa Saadi Mezher received a B.Sc. in Software and Computer Engineering from the Mustansiriyah University (2002-2003), she received an M.Sc. in Computer Engineering from the University of AL Nahreen (2012-2013) and she studying for a Ph.D in Electrical Engineering at the University of Baghdad. She published (12) papers and supervised B.Sc. Her field of interest and her research works focus on Network, Intelligent Methodology, Soft Computing, Neural Networks, Control, Robotics, Computer Architecture, Wireless Sensors, IoT. She can be contacted at email: leqaa.saady2302p@coeng.uobaghdad.edu.iq , iqa35@uomustansiriyah.edu.iq