Blockchain-Enabled Vehicle Documents Verification System

[1]Zohaib Ahmed, [2]Salal Bashir, [1]Barkat Ullah

[1]University of Engineering and Technology, Lahore

[2]Bahria University, Lahore

Corresponding author: Barkat Ullah(barkatullah@usa.edu.pk)

Abstract: - Vehicle documents are evidence of vehicle ownership, thus it's very important for any vehicle owner. Now, a day there are many ways to temper the original vehicle document or create a fake new one. However, the verification of vehicle documents using conventional methods is very time-consuming and costly. In this testing paper, new vehicles have proposed a model for vehicle verification. Using blockchain technology. Our proposal solution has two steps. First the assurance of the vehicle documents in this pace, a document created after the verification of the owner which then passes to the issuing. Department and verified department to sign the vehicle documents digitally, one by one, we have used a multi-sizing algorithm using G-DSA for this purpose after the consensus Process, this vehicle document issued to the owner is in the digital format. The second step is the verification process in which the uploaded documents need to be verified. Vehicle document verification is taken as a case study for this research work. Our proposed model meets all the modifications necessary for modern vehicle document verification in the system. Anyone from anywhere in the world can easily verify vehicle documents by using blockchain-enabled VDVS.

Keywords: Vehicle Document Management System VDVS, Blockchain Technology, SHA-3

1 Introduction

It's easy to register vehicles these days and it's not easy for the issuing department to track the engine number and chasing number. But still, they do issue the original paper to the owner, anyone can use any kind of car from any company just need a little bit of modification it's a tough job for the department to check the originality of the document because there is as we are under development country, we don't have enough resources to check it. And in the case of any murder or robbery when this kind of vehicle is used it is a very tough job for the department to case and verifies the owner of the vehicle.

In the context of the cases quoted above, now we should realize the grandness of a proper, transparent, and fair vehicle Document verification system. The authenticity of a document is not only important for the issuing authority y but is also very important for the document owner. In this modern era, there are many tools available to temper the original documents; this could be difficult for the document owner and issuance authority. It is also becoming more challenging for the owner to verify the authenticity of his vehicle's documents; first, we will discuss some of the major issues that how the stakeholders are facing issues in vehicle document verification and validation, then we will move toward our proposed solutions.

2 Lack of verification mechanism

A person with tempered documents can misuse the vehicles, the owner has no proper mechanism to verify themselves document's originality. The judgment of originality of the hard form of the vehicle's document is very difficult in identifying its signatures. Currently, the owner must send the document code to the excise to validate the ownership of the document; this becomes verse in the scenario if the owner has different vehicles from multiple Departments.

2.1 Loop roles in the existing system

The situation is the same for the vehicle document issuing Departments, in the current scenario departments issue the documents to its customer in hard form, which is very oldfangled, because it could be scanned, copied, tempered easily and so vulnerable to misuse.

As most of the departments are using Management Information Systems to manage, the document records of the customers but still they need to issue the documents in hard form, which is very problematic for the department in that they must keep records of documents in manual form also. It becomes more hectic for the department to issue duplicate documents if required by 50 years old vehicles for example. It is also very difficult for the department to verify the originality of the documents (requested by the customer) by comparing the content with the original one; it is a very time-consuming activity. Similarly, this is very concern able for the document holder if some fake person is misusing his documents.

2.2 MD5 Algorithm

The MD5 message-digest algorithm could even be a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against accidental corruption. It remains suitable for other non-cryptographic purposes, as an example for determining the partition for a selected key during a partitioned database I3J. MD5 was designed by Ronald Rivets in 1991 to exchange an earlier hash. Function MD4,[4] and was laid call in 1992 as RFC 1321. One basic requirement of any cryptographic hash function is that it should be computationally infeasible to hunt out two distinct messages that hash to the same value.

2.2.1 SHA- Family

National Security Agency US had designed SHA-family. It has the following generations:

2.2.2 SHA-0

ln 1993 Secure Hash Algorithm SHA-0 was published. The attacks on this hash algorithm technique show that it is not able to use the algorithm [4].

2.2.3 SHA-1

ln 1995 SHA- I was published. This hash algorithm produces 1 60 bits long hash value against an arbitrary length of the input message. For security reasons and sensitive information protection, this algorithm is not considered to use | 3|. Also, after several successful attacks from 2005 to 2010 Google, Mozilla, and Microsoft had been stopped accepting SSL certificates of SHA- I from 20 l7.

2.2.4 SHA-2

This family is considered as safe because of its different functions name as SHA-224, SHA-5 12, SHA-25 6, SHA-224, and SHA-384. National Institute of ordinary and Technology declared that three functions (SHA-256, SHA-384, and SHA-5 12) of family SHA-2 be termed as SHA-2 after the comparison and testing the safety with the safety of AES and therefore the complexity of security attacking these functions was 2"', 2"' and 2" 'respectively - 1 5 j

The essential hash capacities are the SHA-2 family, which share the equivalent useful structure with some variety within the inward activities, size of the message, size of the block, word estimate, security bits, and message hash estimate, as given in Table 1.

Algorithm Name	**SHA-1**	**SHA-256**	**SHA-512**
Input size	$<2^{64}$	$<2^{64}$	$<2^{128}$
Size of Block	512	512	1024
Word	32	32	64
Size of the Message digest	160	256	512
Security Bits	80	128	256

2.2.4 SHA-3

Keccak-384 is named as SHA-3 hash algorithm. NIST released this Algorithm on August 05, 2005[7]. SHA-3 designed by Guido Bertani, Joan Daemen, Michael Peters, and Gilles Van Asscher. This algorithm is based on the Sponge Function which absorbs the data into the sponge and squeezed the arbitrary length of the output. IOTA node.js library is used in this function. Sponge Construction has three components: A basic function which has a string of fixed length and is symbolically represented by f, a rate parameter r, and a pad principal pad.

2.3 Public/Private Keys

In the symmetric key cryptographic algorithm, both data encryption and decryption use the same key, but asymmetric cryptography deploys dissimilar keys. A public key cryptographic method is used in the form of private key generation for personal use and the public key is used for general use.

2.4 Digital Signature:

A digital signature is based on two types of systems named private-key and public keys. A digital signature based on a public-key has more benefits than a private-key-based digital signature. The RSA (Pins, Shamir, and Alderman, RSA Public Key Encoding Arrangement's discoverer) and digital signature algorithm (DSA) are the most common and popular approaches that are used for public-key. Digital Signature Standard (DSS), published

by NIST. DSS was analyzed in 1991, modified in 1993 with minor changes, and then evolved into the current version with major changes in 1996.

2.5 RSA Approach:

A commonly used plan for digital signature is RSA. The RSA approach is used to sign private key documents. This signed document will be sent to their recipient.1nordertoverifydigitallysigned data content, the recipients have created a new validation key from their verified document, using their public key, and compare the value of the original document with the value of the validation. The authentication and validation of this document are depended on the value of the generated result.

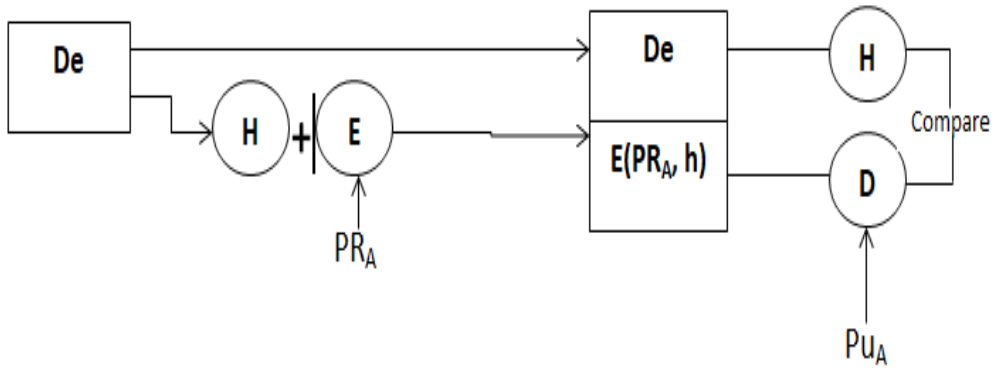

Figure1. RSA

2.6 International needs anti problems

There are too many international organizations in the world, which offer custom-paid and non- custom paid vehicles to their customers; they need to take stress to verify the applicant's document. They too need a system for document investigation. There is no such system for the verification of vehicle documents. 1n our planned solution, we will try to resolve it as well. Due to the lake of proper vehicles documents verification systems, international customers also face problems to validate the customer's vehicle documents.

Keep the above problems into our consideration, we have projected an all-embracing solution for the vehicles document verification system. The solution is based on blockchain technology, and it is new of its kind in providing solutions for vehicle document verification systems in the world. In our proposed solution, we have targeted the security management system for the world. This solution could be available for our entire world.

3 Related Work

A few researchers have designed multiple verification systems by using fuzzy logic [19, 25], soft computing [20], machine learning [21-24], fusion-based approaches [31] using machine learning [26-30, 33-37, 41-47] algorithms, convolutional neural network [32], computational approaches [38-40], Hashing Algorithm, Digital Signature, Multi Signatures, and Block-chain. A few of them are:

3.1-Hash Algorithms

A hash algorithm mortal an input variable into encrypted data, which is unable to understand by humans, only machines can understand this encrypted string known as a hash, which has a fixed extent. As a result, this hash frames a special ID. There are several hash algorithms, that result in a hash production, containing a specific number of digits, based on the type of algorithm. Conducive the same information into the hash generator results in the same hash stream. In any case, even minor changes, in the information input result in a unique hash.

In Figure I, we can see that even a small modification in the input, results in a mismatching hash. Thus, we can use this property of a hash algorithm to identify the tampering or modification in the information and utilize it in a blockchain system for validation purposes.

Different Hash Algorithms are used for information encryption and decryption such as MDS, SHA family (SHA-0, I, 2, and 3), etc.

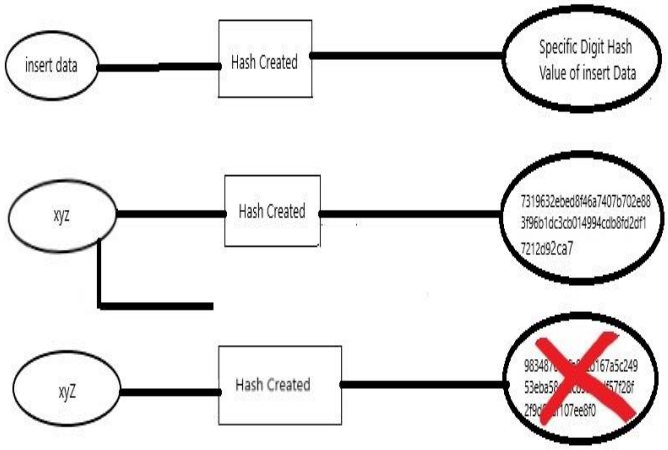

Figure 2. Hash Created

3.2DSS Approach:

General terms and terms in the plural, as well as multivalent concepts, should not be used in the keywords. Be careful in the use of abbreviations: only abbreviations that have been well established in the field of research can suit. These keywords In DSS the signing process is based on Digital signature Algorithm. DSA too deploys hash method process to encrypt the content; this content, then used as an input as first parameter, a random number as the second parameter in a signature method, a Global Element (G) as a third parameter with private key of the sender which produces two elements r' and 's'. At the end, the authentication function uses the signature, hash of the document H(De), public key (Pup) as well as the main global element (C.) and creates a Hash value. A match between the generated hash values and the signature (r) indicates the originality y of the signature. The signature function is that it assures the recipient that only the sender could produce an effective signature with the knowledge of the private key (Pro). This is difficult for DSA scheme to compute discrete algorithms. DSA offers signature function only while RSA can further deliver encryption and key interchange. Signing Verification using RSA is almost 100 times quicker than DSA. The DSA Scheme signature is a bit sharp. The main digital signature plan is working for many mass works such as many parties (group digital signatures), signed by signature organizational, and separately signed by two or more signatures protocol for the contract's agreement, separated by a wide distance.

Figure3. DSS

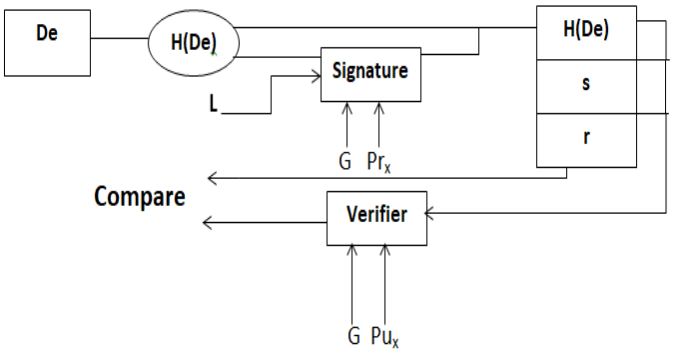

figure3

3.4 multi-Signatures:

It is a digital signature plan multiple users can sign a single document. Generally, multi-signature creates a joint signature compact more than the submission of all the signatures of all users. Multi-signature (often called multiring) is a type of technology used to add additional security to cryptocurrency transactions. Multi-signature addresses require the transaction must be signed before the users are broadcast on the blockchain.

3.5 Block-chain:

The concept of Block-chain merges with other database technology or data. not replace these technologies with the block-chain. Block-chain solution the trustworthiness, mutual consensus, distributive environment, immutability, single point of failure, information security and transparency. Block-chain innovation has opened new uses openings that empower exquisite information partaking in authoritative points of confinement where all associations can oversee themselves and the joined information by. Block-chain appealing for applications multi-party compromise, solid intermediates, and propelled straightforwardness, strength, and honesty. Block-chain application is nor restricted to digital currencies like bitcoin [8], Etherium [9] and one coin (These all system of network of digital currency [11] are running permission less environment), and now its application to be vast in enterprise application.

For recording transactions, block-chain is an immutable ledger, inside a distributed network mutual partners/nodes/peers are internally interconnected. Every node copy of the record. Nodes implement a consensus protocol for transaction validation. This procedure creates a ledger through the transaction setting, for stability. Block-chain has three types, public, consortium. While block-chains are currently popular permissions with [9], Ethernum [10] and other cryptocurrencies, [10] enterprise block-chain applications are emerging, be deployed on production scale soon.

3.5.1 Hyper-ledger Fabric:

The hyper-ledger fabric is a private block [11]. It is a platform that is highly modular and capable, to provide confidentiality, reliability, and sustainability for enterprise blocks. In the mid-2017, with the production of fabric production grade, businesses are using fabric to build real-world block-chain applications. Hyper-ledger Fabric [12] Private (Permission) Blocks Technology is implemented, which is largely based on the promotion of bleach applications for the industry. Therefore, it is built-in module, allows components, such as consent and membership services, plug-ins, and games. It is called "chain-code" which takes the Smart Contract System Technology (Docker) that contains system logic c. It is open source distributed ledger software that is built and maintained by the Hyper-ledger community, which has mutual cooperation, and aims to promote cross-border block-chain technology. [12]

4 Proposed Model for vehicles document issuance and Verification:

We have proposed a comprehensive solution for the vehicle document verification system. Blockchain technology (Hyper-ledger fabric), and new of its kind in providing solutions for vehicle document verification systems. In our proposed solution, targeted a management system for the fake vehicles document system.

In our system, the issuance of vehicle documents from the concerned department. The issuing department creates the document and sends it to the retailer and verifier department with digital signatures. For multi-signing, we used a G-DSA signature protocol, which uses a DSS approach to sign the document digitally, and (t, n) - threshold signature scheme (t-out-of-n) has signing power to the n persons. Threshold signature plan, any group of t persons can sign, but not t, so in our case, we give signing power documents to relevant departments of document issuance, on violation document verifier and valid customer document verification. In threshold signature group of three departments must sign the document. In the protocol round, where each department receives an input, performs levels, and passes it into the output of that account. Three departments are d I, d2, and d3. That is, d2 gets the inputs from the previous department I (in our case it must be the concerned department), run the algorithm, and move to the department along with the message. In the threshold signature, scheme (TSS), although all the nodes have importance regarding security Implementation, the last node is similar to central nodes in terms of functionality y. The role of the first department is to the documents, add a digital signature, and pass the content to the department (d2). In this model, each department plays in accordance with the TSS. The TSS department takes responsibility in such that its different new issuance of the document, so the department's roles are considered stabilized in any way. There are seven rounds.

Round 1

On input the De, d_1

– chooses $k_1 \in_R Z_q$ and computes $z_1 = k_1^{-1} \mod q$

Round 2

At round i = 2, on input the De, $\alpha 1$, $\beta 1$, $\hat{\alpha}_1$, $\hat{\beta}_1$, participant d_i

– abort if $\alpha_1, \beta_1, \hat{\alpha}_1, \hat{\beta}_1 \notin b_E$

– chooses $k_i \in_R Z_q$ and computes $z_i = k_i^{-1} \mod q$

– computes $\alpha_i = z_i \times_E \alpha_{i-1}$ and $\beta_i = (x_i z_i \mod q) \times_E \beta_{i-1}$

– computes $\hat{\alpha}_i = E(z_i)$ and $\hat{\beta}_i = E(x_i z_i \mod q)$

Round 3

At round t = 3 On input the message De, $\alpha_1, \alpha_2, \beta_1, \beta_2, \hat{\alpha}_1, \hat{\alpha}_2, \hat{\beta}_1, \hat{\beta}_2$, participant d_3

– abort if De, $\alpha_1, \alpha_2, \beta_1, \beta_2, \hat{\alpha}_1, \hat{\alpha}_2, \hat{\beta}_1, \hat{\beta}_2 \notin b_E$

– chooses $k_t \in_R Z_q$ and computes $z_t = k_t^{-1} \mod q$

– computes $R_t = G^{k_t}$ in G

– sends R_t to d_{t-1} or d_2

Round 4

At round t +i for i = 1 & t=3 , on input the message R_3, participant d_2

– computes $R_2 = R_3^{k_t^{-i}}$ in G

– sends R_3, R_2 to d_1

Round 5

On input the message R_3, R_2, participant d_1

– computes $R_1 = R_2^{k1}$ in G.

– computes the ZK proof Π_1 which states

* $\exists\ \eta_1, \eta_2 \in [-q^3, q^3]$ such that

* $R_1^{\eta 1} = R_2$ and $G^{\eta 2/\eta 1} = y_1$

* $D(\alpha_1) = \eta_1$ and $D(\beta_1) = \eta_2$

– sends R_1, Π_1 to d_2

Round 6

On input R_1, R_2, Π_1, Π_2 , participant d_2

– computes the ZK proof Π_2 which states

* $\exists\ \eta_1, \eta_2 \in [-q^3, q^3]$ such that

* $R_2^{\eta 1} = R_3$ and $G^{\eta 2/\eta 1} = y_2$

* $D(\alpha_2) = \eta_1 D(\alpha_1)$ and $D(\beta_2) = \eta_2 D(\beta_1)$

* $D(\hat{\alpha}_i) = \eta_1$ and $D(\hat{\beta}_i) = \eta_2$

– sends R_1, R_2 , $\Pi 1$, Π_2 to d_3

– computes $\hat{\mu} = E(z_3)$

– computes $\mu = [(mz_3 \bmod q) \times_E \alpha_2] +_E [(rx_3 z_3 \times_E \beta_2] +_E E(cq)$

– computes the ZK proof Π_3 which states

* $\exists\ \eta_1, \eta_2 \in [-q^3, q^3]$ such that

* $R_3^{\eta 1} = G$ and $G^{\eta 2/\eta 1} = y_3$

* $D(\mu) = m\eta_1 D(\alpha_2) + r\eta_2 D(\beta_2)$

* $D(\hat{\mu}) = \eta_1$ |

– sends $\mu, \hat{\mu}$, Π_2 , Π_3 to all the other departments

Consequently, the security point does not matter exactly how departments are counted and how the departments are given the role. At the en d of the protocol, every department should be proof of each other department. If this validation fails, they will have to confirm these proofs. The departments invited the distributed decryption protocol for the D in comparison to the cipher text. Assume s= D (μ) mod q. Departments as sign for production (r, s.) M.[17]

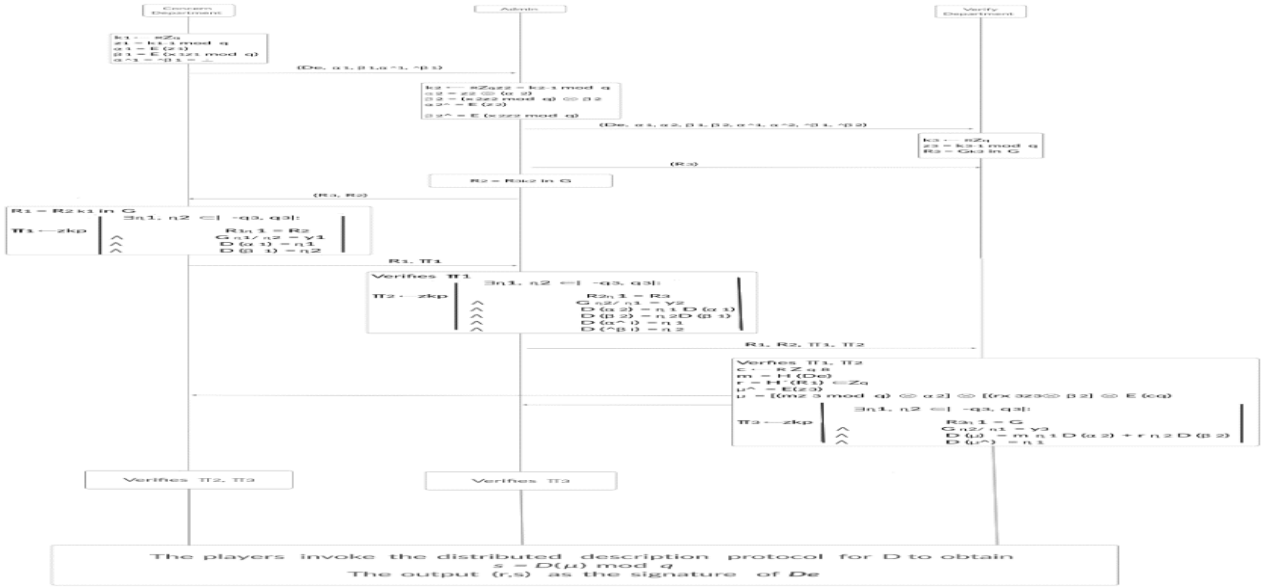

Figure 4

After first step We create the hash of the document (H (De)) using SHA-3, in this *De* is the document to be hashed, and *l* its length in bits where $l < 2^{64}$, then as a first step we create the padded document *De'*. Then *De'* is parsed into *N blocks*. The hash is produced by processing each block De^i of *De'* in order. We create a message schedule W^i. *After the shuffling,* all input blocks from W^i have been used to form a final hash H(De). The output of first step r, s along with H(De) is saved in hyper-ledger fabric after the consensus process. The
document can now be distributed through email or by other means to customer or anyone since it is like the other files. The 2nd Step is the Verification process. We will provide interface, which is accessible for everyone. Anyone can upload the document and verify it. For verification purpose we create the hash of uploaded document H(De) and then check the validity of document by comparing the hash stored in block-chain and the hash of uploaded document. If they are not same, then it can be assumed that the degree may have been changed or the degree was sent by an impostor.

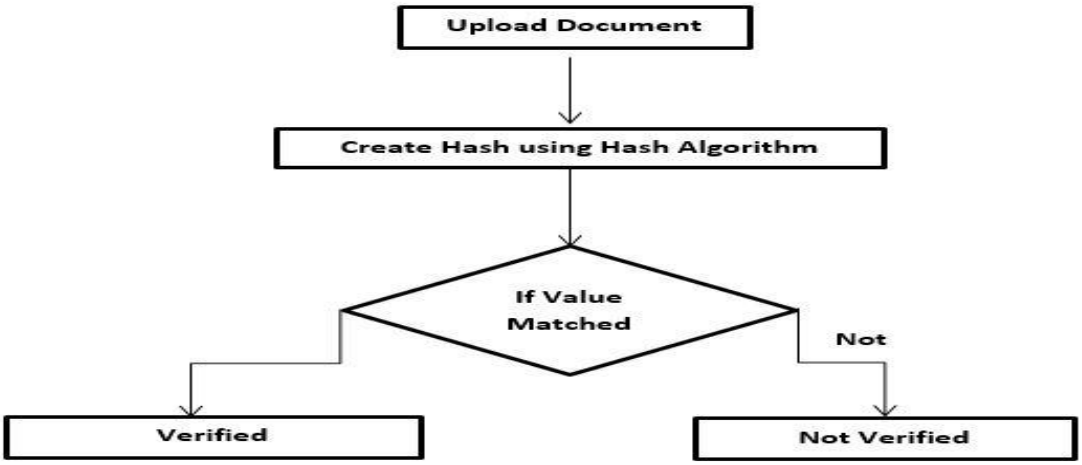

Figure 5

5 Conclusion:

In this paper, we proposed a model of vehicles document issuance and verification primarily for UET using block chain technology and multi-signing algorithm. This model reduces the incidence of tempering, secures the validity of documents and saves time and cost of documents verification. All information providing through our system is valid and immutable due to using private block-chain for saving information. In future, we will implement this model by taking other universities and institutions on board.

6. REFERENCES:

1. O. Ghazal and O. S. Saleh, "A Graduation Certificate Verification Model via Utilization of the Blockchain Technology," vol. 10, no. 3.
2. J. Deepakumara, H. M. Heys, R. Venkatesan, S. J. S, and A. I. B. Canada, "Fpga implementation of md5 hash algorithm," pp. 919–924.
3. K. Järvinen, M. Tommiska, and J. Skyttä, "Hardware Implementation Analysis of the MD5 Hash Algorithm," vol. 00, no. C, pp. 1–10, 2005.
4. L. Chen, "No Title," pp. 1–7, 2011.
5. I. Ahmad and A. S. Das, "Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs q," vol. 31, pp. 345–360, 2005.
6. M. Samet and M. A. B. F. A. Kachouri, "A novel chaos-based image encryption using DNA sequence

operation and Secure Hash Algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, 2016.
7. E. Functions, "FIPS PUB 202 SHA-3 Standard : Permutation-Based Hash and," no. August, 2015.
8. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
9. V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014.
10. M. V. Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers Eran Tromer, "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014.
11. Hyperledger Fabric, "Hyperledger Fabric," 2017.
12. A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat, and S. Chatterjee, "Performance Characterization of Hyperledger Fabric," *2018 Crypto Val. Conf. Blockchain Technol.*, pp. 65–74, 2018.
13. N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, "Enhancing Breeder Document Long-Term Security using Blockchain Technology," 2017.
14. C. F. Bond, F. Amati, and G. Blousson, "Blockchain , academic verification use case," 2015.
15. H. Watanabe and S. Fujimura, "Blockchain Contract : A Complete Consensus using Blockchain," *2015 IEEE 4th Glob. Conf. Consum. Electron.*, pp. 577–578, 2015.
16. M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni, and L. Spalazzi, "Certificate Validation through Public Ledgers and Blockchains," no. November 2011, pp. 156–165, 2017.
17. S. Goldfeder, J. Bonneau, J. A. Kroll, H. Kalodner, and E. W. Felten, "Securing Bitcoin wallets via a new DSA / ECDSA threshold signature scheme," 2011.
18. http://pakistantoday.com.pk.
19. AsadUllah, M., Khan, M. A., Abbas, S., Athar, A., Raza, S. S., & Ahmad, G. (2018). Blind channel and data estimation using fuzzy logic-empowered opposite learning-based mutant particle swarm optimization. Computational intelligence and neuroscience, 2018.
20. Khan, F., Khan, M. A., Abbas, S., Athar, A., Siddiqui, S. Y., Khan, A. H., ... & Hussain, M. (2020). Cloud-based breast cancer prediction empowered with soft computing approaches. Journal of healthcare engineering, 2020.
21. Rehman, A., Athar, A., Khan, M. A., Abbas, S., Fatima, A., & Saeed, A. (2020). Modelling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine. Journal of Ambient Intelligence and Smart Environments, 12(2), 125-138.
22. Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., ... & Ali, A. (2020). A machine learning approach for blockchain-based smart home networks security. IEEE Network, 35(3), 223-229.
23. Khan, M. A., Abbas, S., Atta, A., Ditta, A., Alquhayz, H., Khan, M. F., & Naqvi, R. A. "Intelligent cloud based heart disease prediction system empowered with supervised machine learning," Computers, Materials & Continua, vol. 65, no.1, pp. 139–151, 2020.
24. Khan, M. A., Umair, M., Saleem, M. A., Ali, M. N., & Abbas, S. (2019). CDE using improved opposite based swarm optimization for MIMO systems. Journal of Intelligent & Fuzzy Systems, 37(1), 687-692.
25. Saleem, M., Khan, M. A., Abbas, S., Asif, M., Hassan, M., & Malik, J. A. (2019, July). Intelligent FSO link for communication in natural disasters empowered with fuzzy inference system. In 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (pp. 1-6). IEEE.
26. Ata, A., Khan, M. A., Abbas, S., Khan, M. S., & Ahmad, G. (2021). Adaptive IoT empowered smart road traffic congestion control system using supervised machine learning algorithm. The Computer Journal, 64(11), 1672-1679.
27. Siddiqui, S. Y., Athar, A., Khan, M. A., Abbas, S., Saeed, Y., Khan, M. F., & Hussain, M. (2020). Modelling, simulation and optimization of diagnosis cardiovascular disease using computational intelligence approaches. Journal of Medical Imaging and Health Informatics, 10(5), 1005-1022.
28. Fatima, A., Adnan Khan, M., Abbas, S., Waqas, M., Anum, L., & Asif, M. (2019). Evaluation of planet factors of smart city through multi-layer fuzzy logic (MFL). The ISC International Journal of Information Security, 11(3), 51-58.
29. Hussain, S., Abbas, S., Sohail, T., Adnan Khan, M., & Athar, A. (2019). Estimating virtual trust of cognitive agents using multi layered socio-fuzzy inference system. Journal of Intelligent & Fuzzy Systems, 37(2), 2769-2784.
30. Asif, M., Khan, M. A., Abbas, S., & Saleem, M. (2019, January). Analysis of space & time complexity with PSO based synchronous MC-CDMA system. In 2019 2nd international conference on computing, mathematics and engineering technologies (iCoMET) (pp. 1-5). IEEE.
31. Ihnaini, B., Khan, M. A., Khan, T. A., Abbas, S., Daoud, M. S., Ahmad, M., & Khan, M. A. (2021). A smart healthcare recommendation system for multidisciplinary diabetes patients with data fusion based

on deep ensemble learning. Computational Intelligence and Neuroscience, 2021.
32. G. Ahmad, S. Alanazi, M. Alruwaili, F. Ahmad, M. A. Khan et al., "Intelligent ammunition detection and classification system using convolutional neural network," Computers, Materials & Continua, vol. 67, no.2, pp. 2585–2600, 2021.
33. Hanif, M., Naqvi, R. A., Abbas, S., Khan, M. A., & Iqbal, N. (2020). A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations. IEEE Access, 8, 123536-123555.
34. Saleem, M., Abbas, S., Ghazal, T. M., Khan, M. A., Sahawneh, N., & Ahmad, M. (2022). Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. Egyptian Informatics Journal.
35. Asif, M., Abbas, S., Khan, M.A., Fatima, A., Khan, M.A. and Lee, S.W., 2021. MapReduce based intelligent model for intrusion detection using machine learning technique. Journal of King Saud University-Computer and Information Sciences.
36. F. Alhaidari, S. H. Almotiri, M. A. Ghamdi, M. A. Khan, A. Rehman et al., "Intelligent software-defined network for cognitive routing optimization using deep extreme learning machine approach," Computers, Materials & Continua, vol. 67, no.1, pp. 1269–1285, 2021.
37. Naz, N. S., Khan, M. A., Abbas, S., Ather, A., & Saqib, S. (2020). Intelligent routing between capsules empowered with deep extreme machine learning technique. SN Applied Sciences, 2(1), 1-10.
38. A. H. Khan, M. A. Khan, S. Abbas, S. Y. Siddiqui, M. A. Saeed et al., "Simulation, modeling, and optimization of intelligent kidney disease predication empowered with computational intelligence approaches," Computers, Materials & Continua, vol. 67, no.2, pp. 1399–1412, 2021.
39. Abbas, S., Khan, M. A., Athar, A., Shan, S. A., Saeed, A., & Alyas, T. (2022). Enabling smart city with intelligent congestion control using hops with a hybrid computational approach. The Computer Journal, 65(3), 484-494.
40. Rizvi, S. S. R., Sagheer, A., Adnan, K., & Muhammad, A. (2019). Optical character recognition system for Nastalique Urdu-like script languages using supervised learning. International Journal of Pattern Recognition and Artificial Intelligence, 33(10), 1953004.
41. Hussain, S., Naqvi, R. A., Abbas, S., Khan, M. A., Sohail, T., & Hussain, D. (2021). Trait based trustworthiness assessment in human-agent collaboration using multi-layer fuzzy inference approach. IEEE Access, 9, 73561-73574.
42. Q. Khan, S. Abbas, M. A. Khan, A. Fatima, S. Alanazi et al., "Modelling intelligent driving behaviour using machine learning," Computers, Materials & Continua, vol. 68, no.3, pp. 3061–3077, 2021.
43. N. Tabassum, A. Ditta, T. Alyas, S. Abbas, H. Alquhayz et al., "Prediction of cloud ranking in a hyperconverged cloud ecosystem using machine learning," Computers, Materials & Continua, vol. 67, no.3, pp. 3129–3141, 2021.
44. Ghazal, T.M., Abbas, S., Ahmad, M. and Aftab, S., 2022, February. An IoMT based Ensemble Classification Framework to Predict Treatment Response in Hepatitis C Patients. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-4). IEEE.
45. Abbas, S., Fatima, A., Asif, M. and Saleem, M., Energy Optimization in Smarts Homes by using Fuzzy Inference System.
46. Khan, T.A., Khan, M.S., Abbas, S., Janjua, J.I., Muhammad, S.S. and Asif, M., 2021, April. Topology-Aware Load Balancing in Datacenter Networks. In 2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob) (pp. 220-225). IEEE.
47. Alyas, T.A.T., 2018. Data Breaches Security Issues for Cloud Based Internet of Things. International Journal for Electronic Crime Investigation, 2(1), pp.7-7.