Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.02
Pages: 90-100
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.2.002

Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework

S. Smys,
Professor,
Department of Computer Science and Engineering,
RVS Technical Campus,
Coimbatore, India.
Email: smys375@gmail.com

Haoxiang Wang,
Director and Lead Executive Faculty Member,
GoPerception Laboratory,
Cornell University,
Ithaca, USA.
Email: wanghaoxiang1102@hotmail.com

Abstract: The concept of interconnecting smart vehicles and advancements in automotive automation leads to beneficial outcomes, such as a reduction in road fatalities and congestion. However, including a chain of automation in the attack surface will expand the attack surface and expose the security of automobiles to malicious infiltration. The proposed methodology provides access to specific users while restricting the third party requests. Moreover, it also makes use of data exchange that takes place between the roadside units and vehicle to track the vehicle status without compromising the in-vehicle network. To ensure a valid and authentic communication, vehicles with a proper and verifiable record will only be allowed to exchange messages in the blockchain network. Using qualitative arguments, we have identified that the proposed work is resilient to identified attacks. Similarly, quantitative experimentation indicates that this methodology shows a storage size compatibility and suitable response time in realistic scenarios. Simulation results indicate that, the proposed work shows positive results to secure vehicular networks, vehicular forensics and trust management.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

Keywords: Challenge-response, electronic control units, integrity, vehicular network, blockchain

1. Introduction

The automotive industry has expanded and improved dramatically as a result of technological advancements. Electronic control units (ECUs) enable vehicles to make independent decisions and have improved functionality in modern automobiles, which are no longer just mechanical devices. In order to perform the assigned tasks, ECUs perform computational operations on the inputs received from the sensors. These automobiles are also built with more communication and sensing technologies that have the ability to make decisions. However, this advancement in automobiles has leveraged a negative impact in terms of exploitation of the vehicle. The ECUs can be compromised when faced with malicious attacks, wherein the alluring attackers intend to control the internal network of the vehicle. Communication that takes place between the vehicle and RSUs are known as the internal network of vehicles. This is generally an indicator of on-board buses like the controller area network (CAN). Exploitation of connected and autonomous vehicles is demonstrated in [1] and [2], giving the attackers malicious entities to obtain a complete control over the vehicle. Authors in [3] conducted an extensive research on smart vehicles to understand their vulnerability and the risk imposed under threats and attacks. Based on the impact of the threats on the vehicles, they were categorized into many types by using the threat vulnerability risk assessment technique. This proposed work presents a number of mitigation measures that can be taken to prevent ECU exploitation by properly tracking ECU such that an alert is triggered, when it is compromised.

2. Related Work

A number of security solutions have been proposed for vehicular networks. Trust management, reputation, privacy preservation and automotive network security are some of the solutions put forth by multiple authors. Though vehicular networks have enhanced security due to the generated solutions, they don’t focus on determining the ECU, which has been compromised to provide access to the vehicular networks. Authors in [4] have used a

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

novel message location accountable system that is used to enhance the communication security. However, the reliability of data communication is not considered, which could impose a serious threat in compromising the vehicle network operation. Similarly, the authors in [5] have introduced the blockchain based architecture to enable network security. However, the insider attacks' impact on the architecture is not investigated and this might trigger malicious attacks to be executed by authorised entities. Moreover, veracity of data is not taken into consideration in this work. Security platform for autonomous vehicles has been introduced in [6-8] which don’t report the possibility of application in practical scenarios. This methodology also makes use of a centralised intrusion detector to prevent unauthorised network entry and the subject to single point of failure attack. The authors have not taken into consideration the malicious tenancies of unauthorised entities. Authors in [9] introduced a reputation management and incentive announcement scheme with privacy prevention using Blockchain for the smart automobiles. In this research work, more than one vehicle is used to send a message and this message is verified [16] by all the vehicles before being sent to the roadside unit nearby. Apart from the possibility of collusion attacks, the use of blockchain in the privacy of smart vehicles requires large storage and scalability constraints. Authors in [10] have surveyed and analysed the various factors required for privacy preservation and the privacy issues faced by smart vehicles. Blockchain-based solutions that already exist have also been discussed and a comparative survey is made on the existing privacy preservation methodologies used. They have not taken into account the integrity of in-vehicle sensors and security of in-vehicle networks which are responsible for developing the information that is to be communicated. A novel privacy preservation data integrity checking methodology is proposed by authors in [11] using blockchain exchange. Multi-party verification is used to assess integrity of a system and focus is on preservation of data in the cloud [12-15].

3. Proposed Work

3.1 Architecture of the Proposed Work

Figure 1 describes the architecture of the proposed security measures. This architecture outlines various entities that interact to exchange information and the framework in which they work. This includes the following entities:

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

- Challenge response transaction- how electronic component unit integrity checks are carried out
- Update transaction- how the ECUs are updated
- Genesis block- how the record for a vehicle is created.
- Genesis transaction- how vehicle is registered to a network

There is need for a continuous system to monitor the behaviour of a vehicle and to keep track of the changes that occur in the ECU state. Hence the proposed framework is divided into two tires namely lower tier and upper tier.

The 2 tiers define the role of the entities and make sure that the privacy of the data is preserved. The upper tier is made up of road transport authorities, legal authorities, insurance companies, service technicians and vehicle manufacturers. Since these services are well integrated, it is simpler to keep track of actions like updating [17, 18] which affects the ECU and verification of the ECU state change is possible by the legal and transport authorities who are the only trust entities. In this tire, concentration is on maintenance and vehicle registration. A new block record is created when the vehicle is registered in the upper tier. This includes hash values of these two components and the state of the vehicle. Validation of the vehicle is made using these values with respect to the lower tier [19, 20]. The firmware hashes of the ECU and the current state of the vehicle is compared against the predefined values saved in the lower tier. Similarly, the diagnostic data and schedule maintenance are also stored in the upper tier to keep track of service technicians and vehicle manufacturers. This will play a crucial role in monitoring the vehicle and making liable decisions in testing scenarios [21]. Communication that takes place between the roadside units (RSUs) and the smart vehicles is commonly called a vehicular network. This communication takes place following the standard safety measure as per IEEE 802.11p. When any component of the ECU is compromised, it will pave the way to malicious entity attacks such as false information broadcast that will affect the decisions made by the driver of vehicles.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

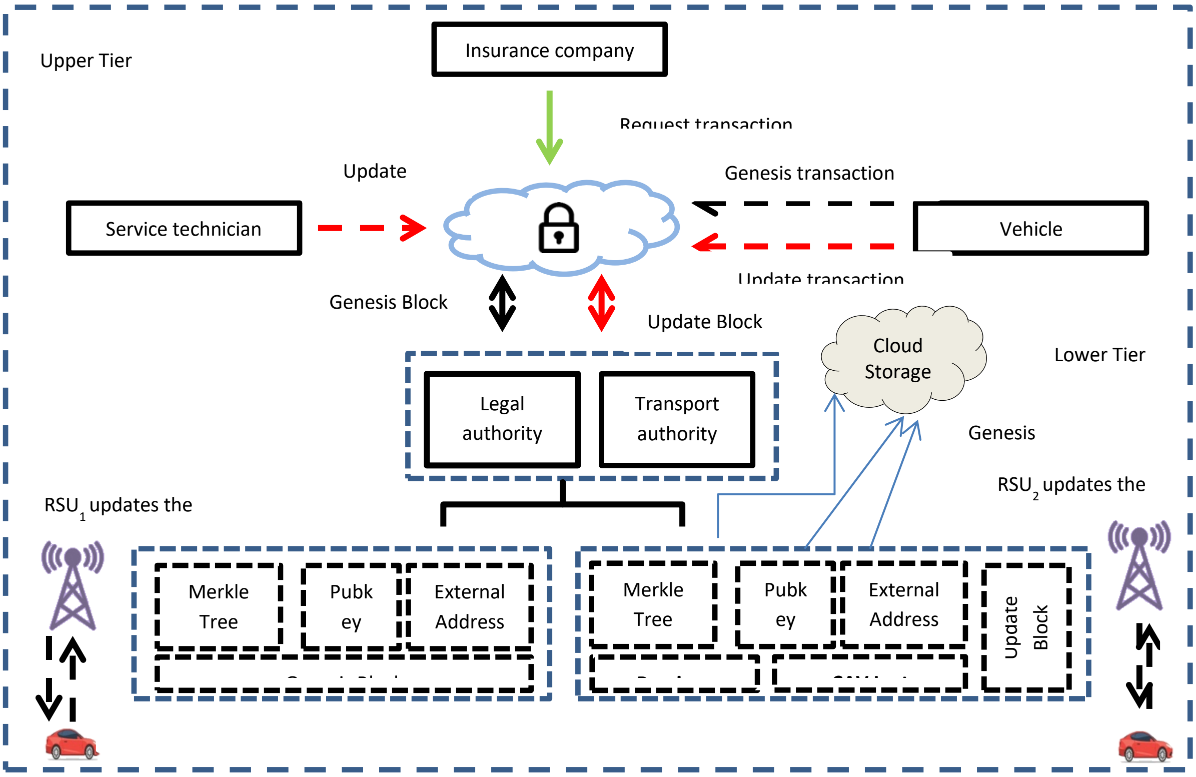

Fig.1. Architecture Framework of the Proposed Work

3.2 Transactions

The basic means of communication that takes place between the smart automobiles and the road side units (RSUs). Information is exchanged during the process of communication which in turn is facilitated by transactions of different types as discussed below:

Upper Tier: Transaction in this layer is inclusive of relevant information on the different actions that are operated on a smart vehicle. It also consists of communication that took place during assembly of the vehicle. In case of an accident, insurance companies could seek for evidence which can be obtained from this tier.

Genesis transactions: During the assembly of the vehicle, the vehicle manufacturer initiates this transaction. It determines the Merkle tree root from the smart vehicle's firmware to determine the hash values such as time stamp, creation time, and other associated timestamps.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

Update Transaction: This transaction is triggered by either service technician or by the vehicle manufacturer. While updating the firmware, this transaction is initiated at the time of diagnostics and maintenance. This will affect the hash values of the components along with the public key and timestamp. When the upper tyre receives an update on transaction, the block or record of the smart vehicle in the lower tyre is also subsequently updated. This updated block is then used for the transactions by the RSU to determine authenticity of the smart vehicle.

Request Transaction: The insurance company initiates this transaction to facilitate compensation payments and liability decisions. This transaction will specifically hold the public key, the data request as well as the signature of the insurance company.

Lower tier: Transactions that take place in the upper tier are reflected in the lower tier and are further appended to their blocks. It is worth noting that the blocks in the upper tier and managed by legal and transport authorities while those in the lower tier are managed by the RSUs. The lower tier communications also provide full information on communication that took place between RSU and smart vehicles.

Block Updating: The legal authorities or the road transport or the RSU update the blocks of the smart vehicle.

- Update transaction is received at the upper tire, blocks updated by the legal authorities and road transport.
- When a challenge request is sent to the smart vehicle blocks updated by an RSU.

Challenge–Response Transaction: To prove that the ECU is not compromised, the RSU issues a challenge-response transaction. The smart vehicle receives this request, when it falls in the area of a RSU. Under such circumstances, the smart vehicle faces the challenge of verifying the identity of its current state and also verifying a random ECU's hash value.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

4. Results and Discussion

A common open research emulator is used to evaluate the performance of the proposed work. The initial experiments are used to determine viability of the project and help to prepare the work for experimentation in real work. To determine the overhead, we have compared the proposed work against a similar database. The observed output is represented graphically in Fig.2, where there is an increase in the time measured, based on the number of vehicles under consideration.

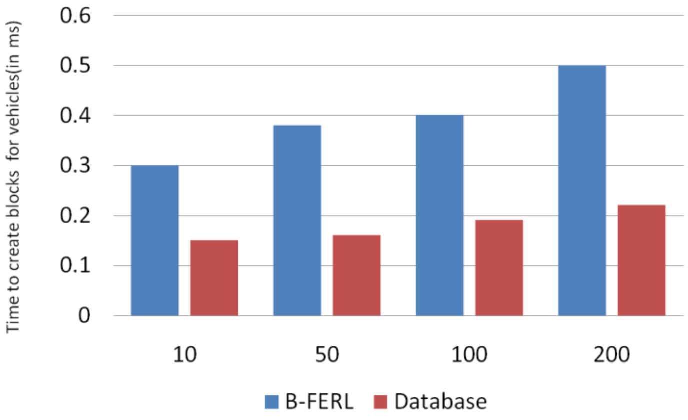

Fig.2. Time Taken for Block Creation

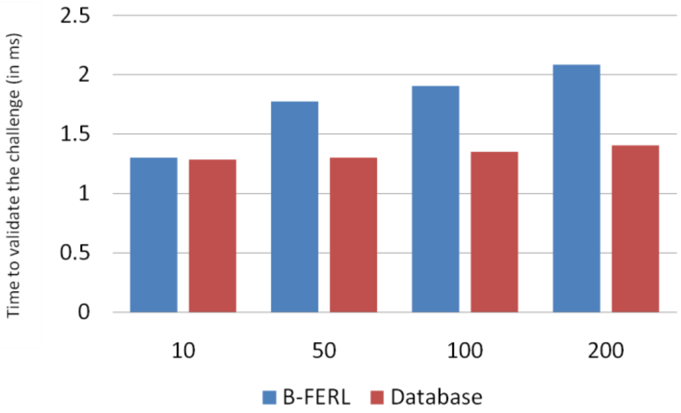

Fig.3. Time Taken for Validation of Blocks

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

When the smart vehicle is registered, a corresponding block is created and the upper tier validators send the information to road side units. Fig. 3 represents the time taken to create a block for the smart vehicle. Based on the number of vehicles to be updated, the time taken will also increase accordingly. Similarly, Fig.4 shows the time taken in order to calculate Merle Time for the smart vehicle and how the components exchange information in the time cycle.

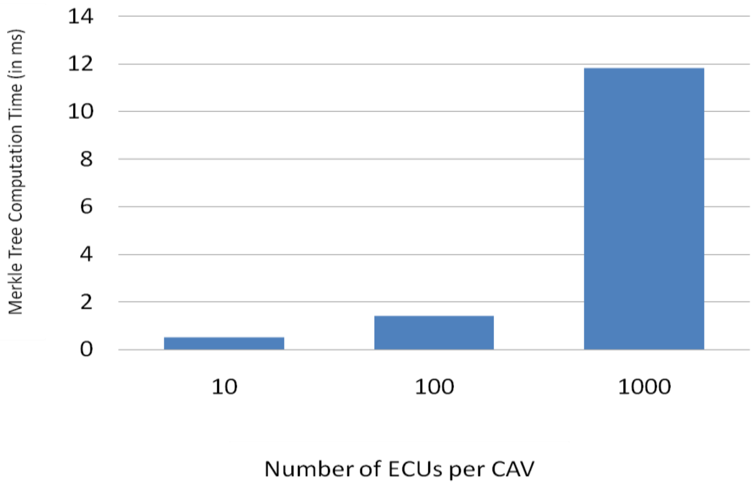

Fig.4. Calculation of Merkle Tree Computation Time

5. Conclusion

The proposed research work has incorporated a secure smart vehicle system using blockchain for framework. The purpose of this paper is to determine when and if electronic component unit (ECU) fails or is compromised by questioning the internal state of the system. If the ECU has been compromised, legal authorities as well as road transport are notified immediately to take preventive measures before the smart vehicle causes any harm. Thus, the proposed work doubles as a reaction and detection mechanism for enhancing the security of the smart automobile. Vehicular forensics, secured vehicular network and trust management are some of the crucial applications that are analysed by using the proposed work and the output records positive evidence of security enhancement. Moreover by evaluating the performance of the proposed work, the challenges faced by smart vehicles are also addressed.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021

Despite the fact that this work provides protection against a variety of attacks, there is still need for improvement in a broad range of attacks, such as those carried out by benign internal entities. Based on the simulation results, we can place on record that this work is applicable in practical scenarios. This paper has identified a flaw, when a vehicle has been compromised to protect the vehicle against possible internal adversaries' exploitation. Interesting future scope will include securing data transmission while communicating data when the smart vehicle moves from a road side unit to the other.

References

[1] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, *55*(12), 119-125.

[2] Adithya, M., P. G. Scholar, and B. Shanthini. "Security Analysis and Preserving Block-Level Data DE-duplication in Cloud Storage Services." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 02 (2020): 120-126.

[3] Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access*, *6*, 13565-13574.

[4] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." Journal of ISMAC 2, no. 02 (2020): 106-117.

[5] Chitra, Ms K., and V. PRASANNA Venkatesan. "An antiquity to the contemporary of secret sharing scheme." Journal of Innovative Image Processing (JIIP) 2, no. 01 (2020): 1-13.

[6] Das, D., Banerjee, S., & Biswas, U. (2021). A secure vehicle theft detection framework using Blockchain and smart contract. *Peer-to-Peer Networking and Applications*, *14*(2), 672-686.

[7] Adam, Edriss Eisa Babikir. "Evaluation of Fingerprint Liveness Detection by Machine Learning Approach-A Systematic View." Journal of ISMAC 3, no. 01 (2021): 16-30.

[8] Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P. K., & Hong, W. C. (2019). Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. *IEEE Access*, *8*, 474-488.

[9] Suma, V., and Wang Haoxiang. "Optimal Key Handover Management for Enhancing Security in Mobile Network." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 181-187.

[10] Singh, M., & Kim, S. (2017). Blockchain based intelligent vehicle data sharing framework. *arXiv preprint arXiv:1708.09721*.

[11] Mugunthan, S. R. "Concept of Li-Fi on Smart Communication between Vehicles and Traffic Signals." Journal: Journal of Ubiquitous Computing and Communication Technologies June 2020, no. 2 (2020): 59-69.

[12] Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. *Journal of Information Security and Applications*, *55*, 102670.

[13] Shirley, D. R. A. (2014, July). Systematic diagnosis of power switches. In *2014 International Conference on Embedded Systems (ICES)* (pp. 32-34). IEEE.

[14] Li, C., Fu, Y., Yu, F. R., Luan, T. H., & Zhang, Y. (2020). Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. *IEEE Transactions on Intelligent Transportation Systems*.

[15] Bestak, Robert. "INTELLIGENT TRAFFIC CONTROL DEVICE MODEL USING AD HOC NETWORK." Journal of Information Technology 1, no. 02 (2019): 68-76.

[16] Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors*, *19*(14), 3165.

[17] Hariharakrishnan, Jayaram, and N. Bhalaji. "Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things." Journal of ISMAC 3, no. 02 (2021): 69-81.

[18] Madaan, G., Bhushan, B., & Kumar, R. (2021). Blockchain-based cyberthreat mitigation systems for smart vehicles and industrial automation. In *Multimedia Technologies in the Internet of Things Environment* (pp. 13-32). Springer, Singapore.

[19] Shakya, Subarna, and Lalitpur Nepal Pulchowk. "The Robust Routing Protocol with Authentication for Wireless Adhoc Networks." Journal of ISMAC 2, no. 02 (2020): 83-95.

[20] Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart City. *Journal of information processing systems*, *13*(1).

[21] Adam, Edriss Eisa Babikir. "Survey on Medical Imaging of Electrical Impedance Tomography (EIT) by Variable Current Pattern Methods." Journal of ISMAC 3, no. 02 (2021): 82-95.

Authors Biography

S.Smys received his M.E. and Ph.D. degrees in Wireless Communication and Networking from Anna University and Karunya University, India. His main area of research activity is localization and routing architecture in wireless networks. He serves as Associate Editor of Computers and Electrical Engineering (C&EE) Journal, Elsevier, and Guest Editor of MONET Journal, Springer. He served as Reviewer for IET, Springer, Inderscience and Elsevier journals. He has published many research articles in refereed journals and IEEE conferences. He has been General chair, Session Chair, TPC Chair and Panelist in several conferences. He is Member of IEEE and Senior Member of IACSIT wireless research group. He has been serving as Organizing Chair and Program Chair of several International conferences and in the Program Committees of several International conferences. Currently, he is working as Professor in the Department of Information Technology at RVS technical Campus, Coimbatore, India.

Haoxiang Wang is currently the director and a lead executive faculty member of GoPerception Laboratory, NY, USA. His research interests include multimedia information processing, pattern recognition and machine learning, remote sensing image processing, and data-driven business intelligence. He has co-authored over 60 journal and conference papers in these fields on journals such as Springer MTAP, Cluster Computing, SIVP; IEEE TII, Communications Magazine; Elsevier Computers & Electrical Engineering, Computers, Environment and Urban Systems, Optik, Sustainable Computing: Informatics and Systems, Journal of Computational Science, Pattern Recognition Letters, Information Sciences, Computers in Industry, Future Generation Computer Systems; Taylor & Francis International Journal of Computers and Applications and conference such as IEEE SMC, ICPR, ICTAI, ICICI, CCIS, and ICACI.

ISSN: 2582-2012 (online)
Submitted: 7.05.2021
Revised: 29.05.2021
Accepted: 14.06.2021
Published: 21.06.2021