AI Based Algorithm-Hardware Separation for IoV Security

Muhammad Naveed Aman
Department of Computer Science
National University of Singapore
Singapore, Singapore
dcsmnam@nus.edu.sg

Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore
Singapore, Singapore
bsikdar@nus.edu.sg

***Abstract*—The Internet of vehicles is emerging as an exciting application to improve safety and providing better services in the form of active road signs, pay-as-you-go insurance, electronic toll, and fleet management. Internet connected vehicles are exposed to new attack vectors in the form of cyber threats and with the increasing trend of cyber attacks, the success of autonomous vehicles depends on their security. Existing techniques for IoV security are based on the un-realistic assumption that all the vehicles are equipped with the same hardware (at least in terms of computational capabilities). However, the hardware platforms used by various vehicle manufacturers are highly heterogeneous. Therefore, a security protocol designed for IoVs should be able to detect the computational capabilities of the underlying platform and adjust the security primitives accordingly. To solve this issue, this paper presents a technique for algorithm-hardware separation for IoV security. The proposed technique uses an iterative routine and the corresponding execution time to detect the computational capabilities of a hardware platform using an artificial intelligence based inference engine. The results on three different commonly used micro-controllers show that the proposed technique can effectively detect the type of hardware platform with up to 100% accuracy.**

***Index Terms*—Internet of Vehicles, algorithm-hardware separation, Security**

I. Introduction

Over the next 10-20 years, vehicle traffic will likely rise to over two billion [1]. Intelligent Transportation Systems (ITSs) and related technologies have played a significant role in this increase with new services such as active road signs, traffic information, pay-as-you-go insurance, electronic toll collection, fleet logistics etc. Adding passengers and self-driving autonomous vehicles to the ITS infrastructure will be the next wave of ITS applications. One and a half million people die each year due to traffic accidents, according to the World Health Organization (WHO). Vehicular communication systems and networks should, therefore, be used for the primary purpose of improving road safety and convenience [2]. The IoV is envisioned as the future of ITSs with over a million vehicles connected to the Internet with autonomous vehicles making up a significant portion of it by 2022.

Although, the IoV may be crucial for realising smart cities, it also introduces new security challenges in the form of cyber threats. Vehicles with communication and sensing capabilities share information including but not limited to speed, location, and acceleration etc. with other vehicles and fixed infrastructure such as road side units (RSUs). Information exchange between vehicles is through vehicle-to-vehicle (V2V) communication, whereas vehicles distribute critical information such as authentication messages and safety-related messages (e.g., an accident occurring within a specific region) through vehicle-to-infrastructure (V2I) links. Therefore, security, privacy, and trust management issues are of utmost importance to the success of IoV. For example, bogus information regarding unsafe or congested road conditions could spread to mislead vehicles, causing a traffic jam. Additionally, modern cars include an internal communication bus system that links together numerous controllers, such as the brakes, airbags, and engine control. An attacker may get access to the internal bus through the external wireless interface of a car and wreak serious harm. Cyber attacks are anticipated to increase by 20.3% in the next decade [3], and because many VANET applications will effect life-or-death choices, network security should be a priority. Thus, autonomous vehicles must be secure before they can be accepted en masse.

One of the major challenges of designing security protocols for the IoV is the heterogeneity and use of proprietary hardware/software in vehicles manufactured by different vendors. Existing security protocols for IoV are based on the implied assumption that all the vehicles in the IoV have same type of hardware and posses the same minimum processing capabilities [4]. However, in practice this may not be the case, i.e., even vehicles from the same manufactures are highly heterogeneous in terms of hardware and software architecture. Therefore, this hard assumption not only makes these techniques infeasible but may also lead to compromise. This paper solves this issue by putting forward the proposal of algorithm-hardware separation, i.e., security algorithms for the IoV designed independently of the hardware or transceiver platform.

This paper focuses on the problem of algorithm-hardware separation for IoV security using artificial intelligence. The proposed technique exploits the computational capabilities of a transceiver to estimate its hardware capabilities. Then, using this information, the proposed protocol adopts the security primitives accordingly. For example, if a vehicle's transceiver does not have the processing power to implement a certain

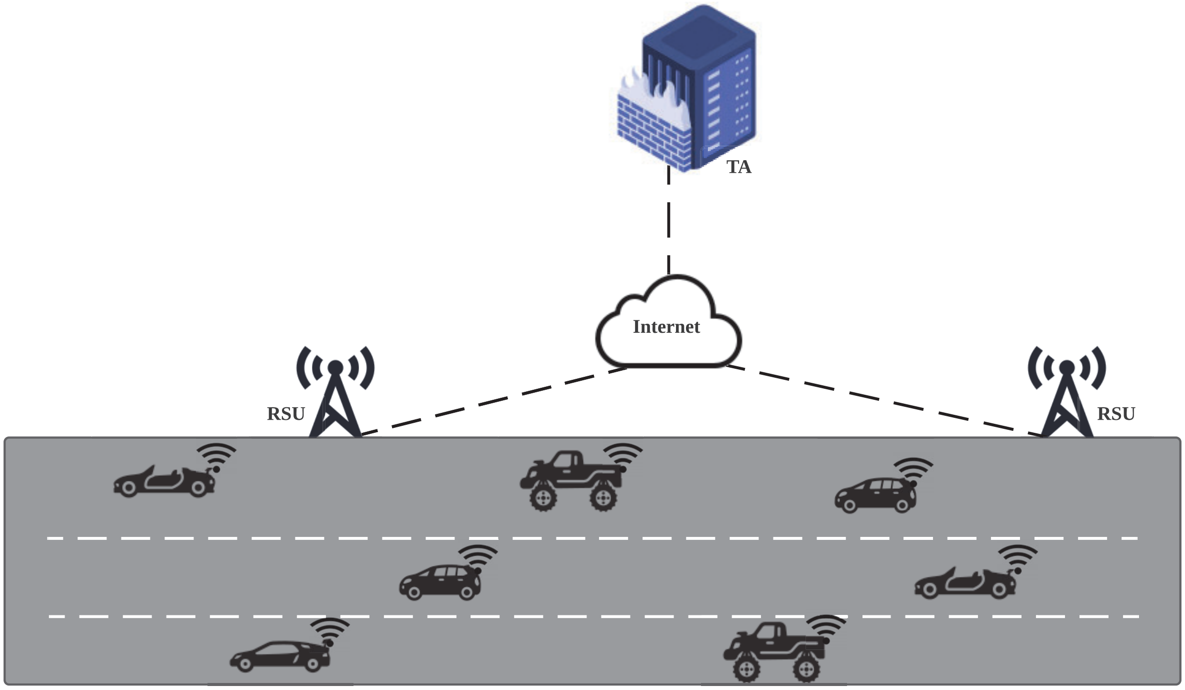


Fig. 1: Network model.

security primitive, then the security algorithm needs to adopt a lower level of security and this information is also conveyed to the other party involved in the communication. Thus, the proposed protocol has two desirable properties in terms of IoV security. That is, if two entities Alice and Bob want to talk to each other, firstly, if Alice's transceiver is not capable of implementing a certain security primitive, then the proposed technique will implement a lighter version of the primitive, leading to better security (as compared to no security without algorithm-hardware separation) and protection of the vehicle's electronics (by avoiding overload or heating). Secondly, the proposed protocol alerts Bob of the lower level of security and consequently Bob can put a correspondingly lower level of trust in the information shared by Alice. The major contributions of this paper are as follows:

(i) Developing the concept of algorithm-hardware separation for IoV security.
(ii) Proposing a mechanism for algorithm-hardware separation using AI.
(iii) Experimental validation of the proposed protocol.

The rest of the paper is organized as follows. A literature review is presented in Section II. Section III describes the network model and assumptions. Section IV presents the proposed algorithm-hardware separation framework for the IoV and Section V describes the use of AI to implement the proposed algorithm-hardware separation framework. Experimental results of the proposed technique are presented in Section VI and the paper is concluded in Section VII.

II. Literature Review

Some of the recent state-of-the art techniques based on public/private key cryptography for IoV security include Fuentes et al. [7], Adigun et al. [8], Whyte et al. [15], and Salem et al. [10], Aman et al. [11], Alladi et al. [12], [13]. A Hashed-Chain based Authentication protocol (HAP) for user validation in VANETs was proposed by Sulaiman et al. [14]. Recent techniques for data provenance in the IoV include the use of digital signatures and elliptic curve cryptography [7], [9]. However, all these techniques make the same assumption of homogeneity, i.e., all vehicles are equipped with the same hardware.

A technique for secure sharing and storage of data using a consortium blockchain for VANETs was proposed in [16]. In their proposal, they present a vehicle identity authentication scheme that asks vehicles to provide identity verification before allowing data sharing. Although intriguing, using a blockchain increases overhead and doesn't scale well. The authors in [17] explore software-defined networking for vehicle-based social networks, where the virtualized network allows transactions to be verified, as well as preserving data integrity, via vehicle authentication. PoolCoin, a Distributed Trust Model for Reputation Management of users in a Network is proposed by the authors in [18]. Their concept can be used to explore the potential for outsourcing the RSU computational load to other interested parties. Javaid et al. [21] and Yang et

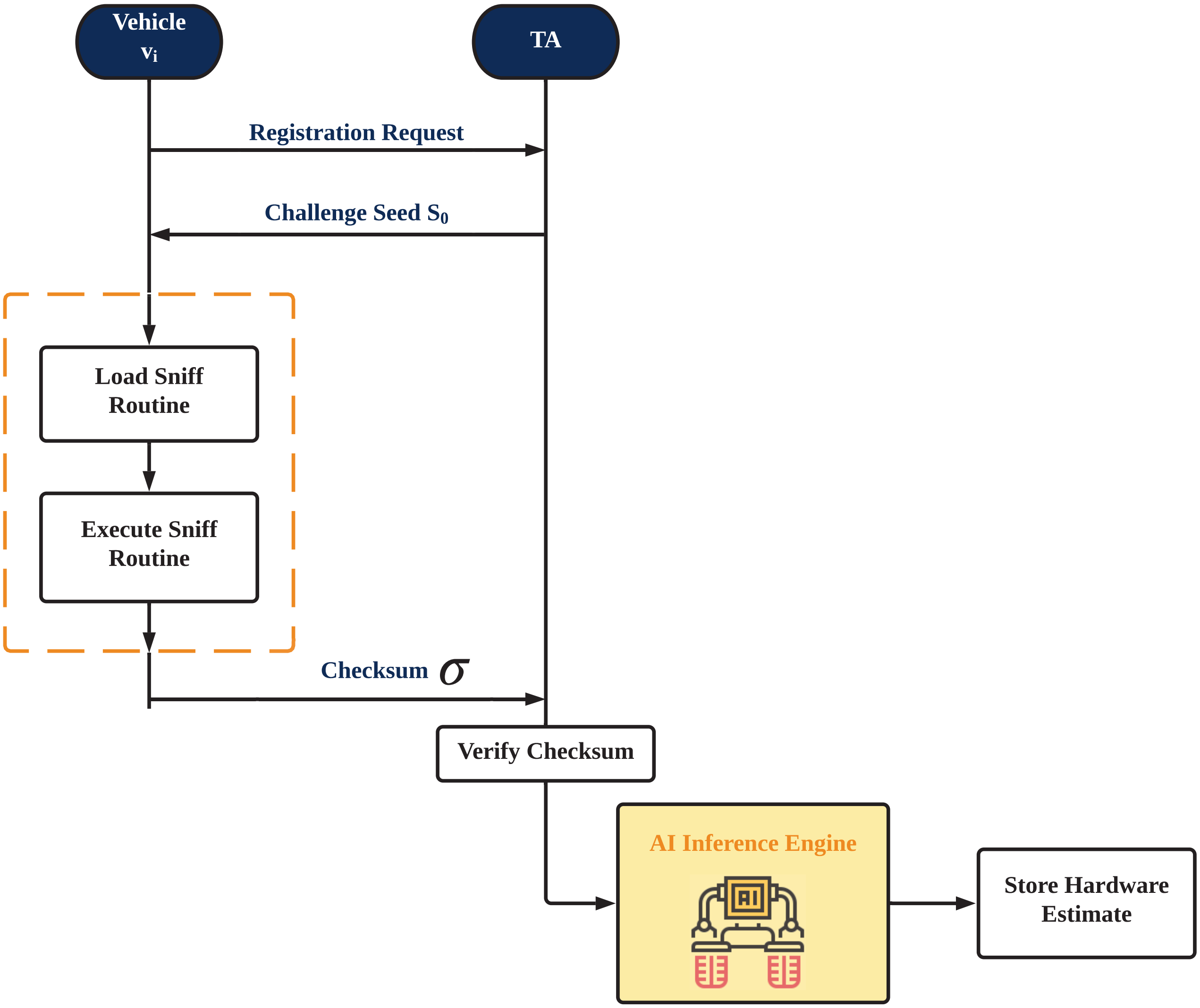


Fig. 2: Proposed framework.

al. [19] use a blockchain to authenticate vehicles in a trust management protocol for VANETs. Finally, Lei et al. [20] found that dynamic key management is necessary for systems with heterogeneous vehicular components. Blockchain is used in their key management protocol, like [19].

This shows that all the existing work on IoV security is based on the assumption of homogeneous hardware for all the vehicles which is contrary to the actual market situation [22]. Therefore, this paper proposes a technique to identify the hardware capabilities of a vehicle so that the security primitive that it can support can be chosen accordingly. To the best of author's knowledge, this is the first work on algorithm-hardware separation for IoV security.

III. System Model

A. Network Model

The network model considered in this paper is shown in Figure 1. We consider a set of vehicles $\mathcal{V} = \{v_1, v_2, \cdots, v_n\}$ connected to the Internet and RSUs serving them. The RSUs are in turn connected to a central authority termed trusted authority (TA). It is assumed that the vehicles can communicate with each other as well as the RSUs.

B. Assumptions

The following assumptions are made:

i) The vehicles are considered to be heterogeneous in terms of their computational capabilities.
ii) The RSU is not constrained in terms of computational capabilities or energy.

iii) No assumptions are made regarding the physical layer protocol used.
iv) The vehicles are not constrained in terms of energy.

IV. Proposed Algorithm-Hardware Separation Framework for IoV Security

The proposed framework for algorithm-hardware separation is shown in Figure 2. When a vehicle wants to communicate with another vehicle or RSU, it needs to register itself with the trusted authority (TA). The steps of this protocol are as follows:

1) On receiving a registration request from a vehicle, the TA sends a challenge seed S_0 to the vehicle.
2) The vehicle then loads a `Sniff` routine which calculates a checksum using the challenge seed S_0.
3) The resulting checksum σ is returned back to the TA.
4) After verifying the checksum σ, the TA inputs the execution time into the proposed AI inference engine described in Section V.

The `Sniff` routine can by any iterative algorithm, whose completion time depends on the computation power of the platform it is running on [5], [6]. The `Sniff` routine used in this paper is given in Algorithm 1. This algorithm makes a large number of iterations over the memory of a vehicle's transceiver and calculates a hash digest. Note that in Algorithm 1, `PRNG` represents a pseudo-random number generator. The steps of the proposed `Sniff` routine are as follows:

1) Calculate the initial checksum σ_0 by generating a pseudo-random number (PRN) using S_0 as the seed.
2) For a large number of iterations (typically at least 50,000):
   a) Generate a PRN using the previous checksum value σ_{i-1} as the seed.
   b) Calculate the new checksum value σ_i by taking the hash of the PRN generated in the previous step.
3) Return the last checksum value σ_N.

Algorithm 1: Proposed `Sniff` routine.

```
function Sniff($S_0$)
Input : $S_0$
// Challenge Seed
Output: $\sigma$
$\sigma_0 = \mathtt{PRNG}(S_0)$
for $i \leftarrow 1$ to $N$ by $1$ do
    $\sigma_i = \mathtt{H}(\mathtt{PRNG}(\sigma_{i-1}))$
return $\sigma_N$
end function
```

V. AI based Hardware Sniffing

In this section, we present the proposed technique to identify a hardware platform using the execution time of the `Sniff` routine as the predictor. The overall process of training our AI inference engine is shown in Figure 3. To train the inference engine, the steps in Figure 3 are carried out for each hardware platform that we consider. n_{iter} represents the number of observations in the training data, in each iteration, a new random seed (generated using a PRNG) is used to execute the `Sniff` routine on the target platform and measure the execution time. Then, labelled data is used to train a machine learning based classifier.

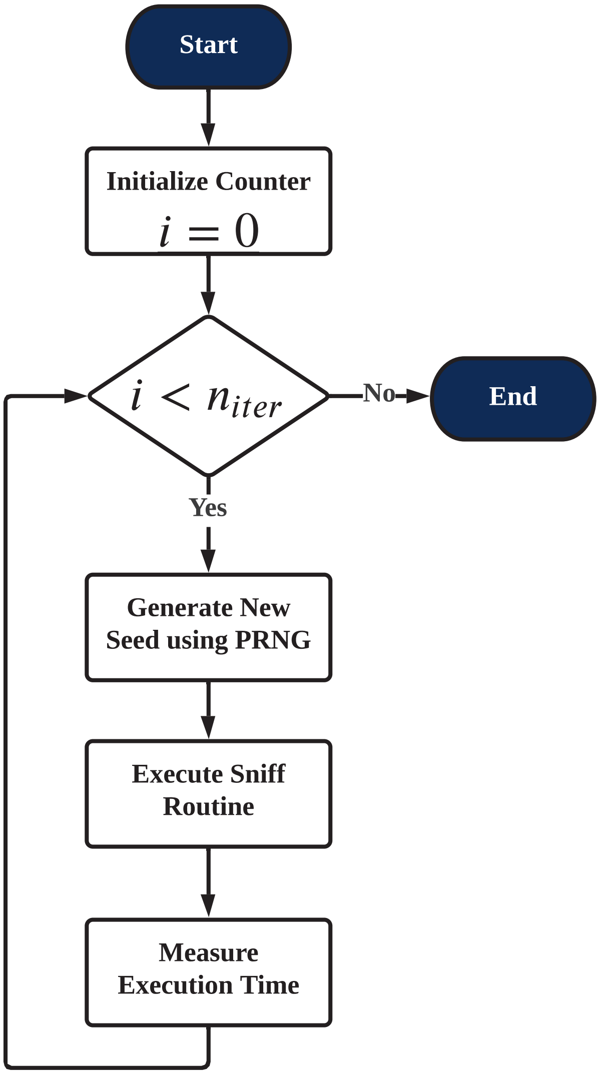
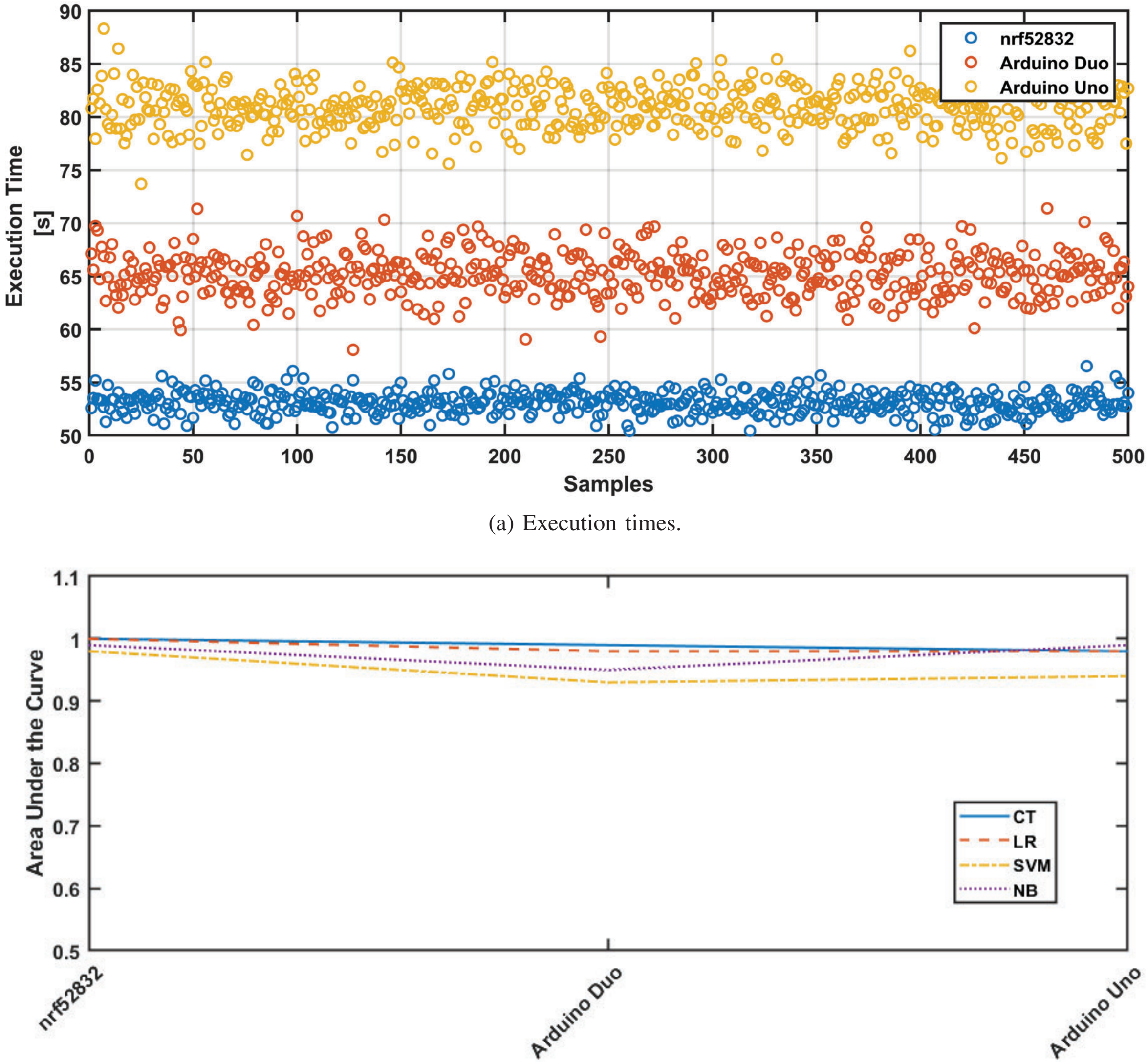


Fig. 3: Training the proposed AI inference engine.

VI. Results

To present a proof of concept, we used three different commonly used micro-controllers (mcu) given in Table I. The execution times plotted after collecting 500 samples for each platform are shown in Figure 4(a). We observe that the execution times for the three platforms with different architectures are clearly separated. We trained the following four different machine learning classifiers using this training data set: classification trees (CT), logistic regression (LR),



(a) Execution times.

(b) AUC using different classifiers.

Fig. 4: Experiment results – $n_{iter} = 50,000$.

support vector machines (SVM), and Naive Bayes (NB). To assess the performance of these classifiers Figure 4(b) presents the area under the receiver operating characteristic curve (AUC). We observe that classification trees outperform the other classifiers. Moreover, the AUC is close to 1.0 which shows that the proposed technique can be used to identify hardware platforms with high accuracy.

Platform	Architecture	SRAM
nrf52832	ARM Cortex M4	64 KB
Arduino Duo	ARM Cortex M3	96 KB
Arduino Uno	AVR	2 KB

TABLE I: Platforms used in experiments.

VII. Conclusion

A technique to implement algorithm-hardware separation for IoV security was presented. The proposed technique uses a `Sniff` routine to exploit the hardware computational capabilities of the underlying platform and using the execution times can effectively identify the hardware platform. An artificial intelligence based inference engine was trained using various machine learning techniques based on execution time as the predictor. Experimental results on three different commonly used hardware platforms showed that the proposed technique can identify the hardware platform with upto 100% accuracy.

References

[1] D. Jia, K. Lu, J. Wang, X. Zhang and X. Shen, “A Survey on Platoon-Based Vehicular Cyber-Physical Systems,” in *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 263-284, Firstquarter 2016.

[2] Mejri, M.N., Ben-Othman, J., and Hamdi, M., “Survey on VANET security challenges and possible cryptographic solutions.” *Veh. Commun.*, vol. 1, no. 2, pp. 53-66, Apr. 2014.

[3] Global Risks 2015 Report.10th Ed., World Economic Forum, Geneva.

[4] Surbhi Sharma, Baijnath Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions.” in *Vehicular Communications*, Vol. 20, 2019.

[5] M. N. Aman, B. Sikdar, “ATT-Auth: A Hybrid Protocol for Industrial IoT Attestation With Authentication,” in *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5119-5131, Dec. 2018.

[6] M. N. Aman et al., “HAtt: Hybrid Remote Attestation for the Internet of Things with High Availability,” in *IEEE Internet of Things Journal*, 2020.

[7] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, “Overview of security issues in Vehicular Ad hoc Networks.” *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, 2010.

[8] A. Adigun B. A. Bensaber, and I. Biskri, “Protocol of change pseudonyms for VANETs.” Proc. 3rd Annual DIVA Workshop”, *NSERC DIVA workshop*, 2013, pp. 150-155.

[9] IEEE Standards Association, “IEEE guide for wireless Access in vehicular environments (WAVE) architecture,” 2013.

[10] A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, “The case for dynamic key distribution for PKI-based VANETS,” *International journal of Computer Networks & Communications*, vol. 6, no. 1, pp. 61–78, Jan. 2014.

[11] M. N. Aman, U. Javaid and B. Sikdar, “A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles,” in *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123-1139, 15 Jan.15, 2021.

[12] T. Alladi, S. Chakravarty, V. Chamola and M. Guizani, “A Lightweight Authentication and Attestation Scheme for In-Transit Vehicles in IoV Scenario,” in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14188-14197, Dec. 2020.

[13] T. Alladi, V. Kohli, V. Chamola and F. R. Yu, “Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework,” in *IEEE Networking Letters*, vol. 3, no. 2, pp. 94-97, June 2021.

[14] A. Sulaiman, S. V. Kasmir Raja, and S. H. Park, “Improving scalability in vehicular communication using one-way hash chain method,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2526–2540, Nov. 2013.

[15] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A security credential management system for V2V communications,” *in Vehicular Networking Conference (VNC)*, 2013 IEEE, 2013, pp. 1–8.

[16] X. Zhang and X. Chen, “Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network,” in *IEEE Access*, vol. 7, pp. 58241-58254, 2019.

[17] Y. Yahiatene and A. Rachedi, “Towards a Blockchain and Software-Defined Vehicular Networks Approaches to Secure Vehicular Social Network,” 2018 *IEEE Conference on Standards for Communications and Networking (CSCN)*, Paris, 2018, pp. 1-7.

[18] A. Kaci and A. Rachedi, “PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain,” 2020 *IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2020, pp. 1-6.

[19] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, “Blockchain-Based Decentralized Trust Management in Vehicular Networks,” in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495-1505, April 2019.

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832-1843, Dec. 2017.

[21] U. Javaid, M. N. Aman and B. Sikdar, “A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain,” in *IEEE Internet of Things Journal*. vol. 7, no. 12, pp. 11815-11829, Dec. 2020.

[22] “40+ Corporations Working On Autonomous Vehicles.” Available: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/ . Accessed: 04 July, 2021.