Chapter 7
Blockchain–Based Authentication for the Internet of Vehicles (BBA–IoV)

Rida Zehra

https://orcid.org/0009-0009-2468-3970
University of the West of England, UK

ABSTRACT

IoV has become an appealing application that can provide a wide range of mobile services for drivers. In order to mitigate traffic congestion and reduce the occurrence of accidents, vehicles can be provided with up-to-date information regarding the location, trajectory, speed, and other relevant details of adjacent vehicles. Such an open environment leaves a lot of room for malicious nodes to pass falsified and tampered information. Due to the potential relevance and sensitivity of the information, IoV must address the security and privacy concerns in the network. In this chapter, they propose an efficient IoV-based decentralised authentication mechanism based on the blockchain named BBA- IoV to ensure secure node communication. This method requires the exchange of keys to encrypt communication. From performance analysis, they show that this approach protects communication against several attacks such as Sybil, GPS spoofing, tampering, and fabrication attacks.

IoV is a transformation of Vehicular Ad Hoc Networks (VANETs) that can increase traffic efficiency. The evolution of sensing and communication technologies and their rapid usage in vehicular communication has made it possible for vehicles to connect with other road infrastructures to convey information in real time (Jiang et al., 2019). The growth of the Internet of Things (IoT) allows vehicles to be self-

sufficient and smarter and provides a platform to enable the IoV. According to (Li, 2012), the number of vehicles globally could rise to between two and five billion by 2050.

There are two main types of VANET communications, namely Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure(V2I) (Fangchun et al., 2014). Communication between vehicles in the IoV is possible, as well as with pedestrians, signs, and roadside units (Nakamoto, 2009). The communication can be related to route planning, road congestion, traffic issues, and emergency details that need to be secure; for example, the actual identity of a driver must not be disclosed.

In a rapidly evolving world where vehicles are becoming more interconnected, there are various security and privacy concerns that pose risks to the safety of drivers and passengers. These concerns include data manipulation, authenticity, and the potential disclosure of sensitive information. Thus, vehicles in the IoV are vulnerable to security threats by presenting false information that leads to serious risks; it is, therefore, necessary to fix these problems. In current studies such as (Aich et al., 2019; Leo et al., 2020; Qu et al., 2015), proposed methods are highly centralised, which means a single point of failure can damage the whole system -if the central authority is targeted data will be maliciously exploited -needs to be resolved. This issue is where the blockchain has been proposed and advocated as an adequate solution.

Blockchain is a decentralised ledger that employs a distributed data structure comprised of a sequential chain of blocks to store transaction information. The objective is to streamline peer-to-peer (P2P) transactions by eliminating the requirement for direct interactions between peers and any involvement from intermediaries. Several studies have explored the use of blockchain as a solution for vehicle authentication methods, such as (Al Ameen et al., 2012), whereby a blockchain-based authentication system seeks to solve centralised infrastructure, anonymity, and trust. They proposed a lightweight authentication system for automotive fog infrastructure. Similarly, an authentication system for vehicles using blockchain based on the services of fog was implemented in the paper (Sharma et al., 2018). The existing works mentioned above do not discuss integrating blockchain to provide authentication to both vehicle and service management. We present a novel architecture for the integration of blockchain into existing vehicular systems.

They, therefore, suggested an improved new approach to avoid the issue of authentication with blockchain technology. The use of blockchain technology has several benefits, including any vehicle can enter the block and can confirm that other vehicles are authentic without any third party. In the field of protection, safety, and performance, the integration of blockchain and IoT will potentially improve the current IoV network. The BBA-IoV method includes encryption techniques for generating and exchanging keys to ensure security. The RA is the transport

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/blockchain-based-authentication-for-the-internet-of-vehicles-bba-iov/341418

Related Content

Defining Cyber Weapon in Context of Technology and Law
Prashant Mali (2018). *International Journal of Cyber Warfare and Terrorism (pp. 43-55).*
www.irma-international.org/article/defining-cyber-weapon-in-context-of-technology-and-law/198318

Attribution
Clement Guitton (2015). *Cybersecurity Policies and Strategies for Cyberwarfare Prevention (pp. 37-60).*
www.irma-international.org/chapter/attribution/133925

Situation Understanding for Operational Art in Cyber Operations
Tuija Kuusisto, Rauno Kuusistoand Wolfgang Roehrig (2016). *International Journal of Cyber Warfare and Terrorism (pp. 1-14).*
www.irma-international.org/article/situation-understanding-for-operational-art-in-cyber-operations/152644

Assessing the Defence Cooperation Agreements Between the USA and African Countries: The Case of Ghana
Paul Coonley Boatengand Gerald Dapaah Gyamfi (2022). *International Journal of Cyber Warfare and Terrorism (pp. 1-14).*
www.irma-international.org/article/assessing-the-defence-cooperation-agreements-between-the-usa-and-african-countries/311420

Role of FS-ISAC in Countering Cyber Terrorism
Manish Guptaand H. R. Rao (2007). *Cyber Warfare and Cyber Terrorism (pp. 83-90).*
www.irma-international.org/chapter/role-isac-countering-cyber-terrorism/7443