

***Subject of thesis:***

***Integrating Big Data and Blockchain Technologies for Securing Data Collected in VANET***

**CONTEXT**

In today's digital world, intelligent transportation system (ITS) plays a very important role in making the life of the citizens easy in every facet. ITS aims to achieve higher traffic efficiency by minimizing traffic problems and controlling unpleasant events. The ITS offers pervasive and robust services in terms of providing road and traffic safeties, reducing traffic congestion and improving traffic flow, and providing entertainment services on the vehicles, etc. Recently, the integration of smart sensing devices into the vehicles has led to a revolution in the transportation and traffic systems. As a result, we witnessed the generation of a new type of networks called as Vehicular Ad Hoc Networks (VANET). Basically, VANET is a special type mobile networks (MONET) with road routes, which depends on registration mechanism, roadside units (RSUs), and onboard units (OBUs). The OBUs are the radios that are installed in every vehicle as a transmitter to communicate with each vehicle, while RSUs are installed along the street with network devices. RSUs are used to communicate with the infrastructure and contain the network devices for dedicated short-range communication (DSRC). VANETs are classified into two categories: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The main responsibility of VANETs is to produce effective communication; basically, the nodes require specific features to acquire information, to communicate with the neighbors, and then to take decisions based on all information collected by using sensors, cameras, global positioning system (GPS) receivers, and omnidirectional antennas.

**BUT**

Despite their advantages, the sustainability of VANET is subject to numerous potential risks in safety and performance, such as control malfunction and low energy efficiency. Besides, the connectivity in such networks becomes a growing concern due to the complexity of the transportation system. The state-of-the-art VANET faces issues in their large scale deployment in real-world applications, it is due to the following challenges in these architectures:

**System Performance:** the salient features of VANET (e.g., varying node density, high mobility) makes it challenging to coordinate VANETs to efficiently provide services with diverse Quality of Service (QoS) requirements. Indeed, the data collected in VANET are characterized by its massive size, high speed generation, and diversity (numerical, images, and videos). Unfortunately, such characteristics provide several challenges for data analysts and decision makers; first, the traditional data warehousing systems cannot store such amount of big data streaming. Second, data processing is another challenge in transport systems due to the huge computation power needed to handle such amount of data. Third, data analysis is a very complicated task because much of the generated data is of no interest, meaningless and redundant. Hence, the system architecture is becoming key enablers for VANETS to support inter-operation among underlying heterogeneous networks, conduct resource allocation tasks, and effectively manage a vast number of mobile nodes (or users) with heterogeneous smart devices. Recently, the Big Data technologies have been proposed as efficient solutions to overcome the Big data challenges in VANET. Subsequently, the rise of Big data technologies like Hadoop ecosystems allows to build systems based on clusters that use parallel computing. This can ensure a high scalability and reliability of the collected data as well as a fast and huge data storage. In addition, the parallel computing ensures a rapid data processing especially when the volume of data becomes bigger.

**Secure data collection and transmission:** one of the most important challenges in VANET is security. Indeed, VANET has several weaknesses against major security attacks that violates security services such as availability, confidentiality, authentication, and data integrity. Therefore, there are several kinds of attacks that threaten VANET systems including the DDoS, forgery, jamming, impersonation, malware injection, sinkhole, sybil, and replay attacks. Hence, the VANET systems must ensure that the data are collected in a secure manner, thus none of malicious sources/events are happened. Furthermore, security during transmission means that no one should be able to read or change data during along the path to the end user. Therefore, introducing new security and data encryption methods should take a great attention from researchers when dealing with data collected in VANET. Recently, with the emergence of blockchain technology, VANET has tackle a new trend in securing the data and ensuring a high level of confidentiality for the transmitted data. The blockchain technology has led to a revolution in VANET security by providing a distributed security solutions, i.e. the case of mobile vehicles communication, rather than a centrally controlled solution. Thus, with blockchain, there will be no need for a central administrator but all the vehicles are in control of all their information and transactions. Furthermore, since VANET deals with confidential mobile information and requires quick access to information, blockchain can streamline these communicated records and enable their sharing in a secure way.

**EXPECTED WORK**

The first part of the work is to make a state of the art of the VANET systems, Big Data technologies and Blockchain in order to become familiar with the field. The purpose of this part is to study all the issues and challenges related to the VANET as well as existing solutions while focusing on the network architecture, big data collection and security challenges.

In the second part, we are interested in encryption data transmission strategies to secure data generated in VANET networks. It consists of studying, using and adopting artificial intelligence, encryption/decryption methods, and blockchain technology in order to provide a secure data communication between vehicles themselves and between vehicles and RSU.

This work also includes a practical part that consists in applying our proposed mechanisms and platforms in real case scenarios from some transportation cities.

**KEYWORDS**

VANET; Security; Network Attacks; Cryptography; Hadoop Ecosystem; Blockchain, Privacy-Preserving Authentication.

**REFERENCES**

* Arif, Muhammad and Wang, Guojun and Bhuiyan, Md Zakirul Alam and Wang, Tian and Chen, Jianer. **“A survey on security attacks in VANETs: Communication, applications and challenges”**. Vehicular Communications, 19, pp. 100179, 2019.
* Sheikh, Muhammad Sameer and Liang, Jun. **“A comprehensive survey on VANET security services in traffic management system”**. Wireless Communications and Mobile Computing, 2019.
* Sheikh, Muhammad Sameer and Liang, Jun and Wang, Wensong. **“A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)”**. Sensors, 19, pp. 3589, 2019.
* Jaballah, Wafa Ben and Conti, Mauro and Lal, Chhagan. **“A survey on software-defined VANETs: benefits, challenges, and future directions”**. arXiv preprint arXiv:1904.04577, 2019.
* Manivannan, Dakshnamoorthy and Moni, Shafika Showkat and Zeadally, Sherali. **“Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)”**. Vehicular Communications, 25, pp. 100247, 2020.
* Zhang, Xiaohong and Chen, Xiaofeng. **“Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network”**. IEEE Access, 7, pp. 58241--58254, 2019.
* Adhikary, Kaushik and Bhushan, Shashi and Kumar, Sunil and Dutta, Kamlesh. **“Hybrid Algorithm to Detect DDoS Attacks in VANETs”**. Wireless Personal Communications, pp. 1--22, 2020.
* Schmidt, David A and Khan, Mohammad S and Bennett, Brian T. **“Spline Based Intrusion Detection in Vehicular Ad Hoc Networks (VANET)”**. 2019 SoutheastCon, pp. 1--5, 2019.
* Baza, Mohamed and Nabil, Mahmoud and Mahmoud, Mohamed Mohamed Elsalih Abdelsalam and Bewermeier, Niclas and Fidan, Kemal and Alasmary, Waleed and Abdallah, Mohamed. **“Detecting sybil attacks using proofs of work and location in vanets”**. IEEE Transactions on Dependable and Secure Computing, 2020.
* Bhatia, Jitendra and Kakadia, Parth and Bhavsar, Madhuri and Tanwar, Sudeep. “SDN-enabled Network Coding Based Secure Data Dissemination in VANET Environment”. IEEE Internet of Things Journal, 2019.
* Singh, Pranav Kumar and Gupta, Shivam and Vashistha, Ritveeka and Nandi, Sunit Kumar and Nandi, Sukumar. **“Machine learning based approach to detect position falsification attack in vanets”**. International Conference on Security \& Privacy, pp. 166--178, 2019.
* Khan, Uzma and Agrawal, Shikha and Silakari, Sanjay. **“Detection of malicious nodes (DMN) in vehicular ad-hoc networks”**. Procedia computer science, 46, pp. 965--972, 2015.
* Thigale, Somnath B and Pandey, Rahul K and Gadekar, Prakash R and Dhotre, Virendrakumar A and Junnarkar, Aparna A. **“Lightweight novel trust based framework for IoT enabled wireless network communications”**. Periodicals of Engineering and Natural Sciences, 7, pp. 1126--1137, 2019.
* Bhatia, Jitendra and Dave, Ridham and Bhayani, Heta and Tanwar, Sudeep and Nayyar, Anand. **“Sdn-based real-time urban traffic analysis in vanet environment”**. Computer Communications, 149, pp. 162--175, 2020.
* ***More references will be later added.***