JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

VANETS: AN EFFECTIVE AND SECURE SECRET KEY EXTRACTION METHOD BASED ON BLOCKCHAIN

Kavin S [1], Bharathi P [2], Hariprasath S [3] and Dr. G. Singaravel [4]

[1][2][3] Student, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Tamilnadu.

[4] Head of The Department, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Tamilnadu.

ABSTRACT

The greatest progress in resolving the crucial problem of location privacy in Vehicular Impromptu Networks (VANETs), to essential component of Intelligent Traffic Systems (ITS), using innovative block chain-based trust management methodology. VANETs' high inherent mobility has long presented security issues, especially when it comes to using Location-Based Services (LBS). The creative solution gives cars the ability to request LBS while protecting their personal data with a secure verification process. Vehicle privacy is protected via the creation of anonymous shrouding zones, and vehicle behaviour is controlled and governed by an advanced trust management algorithm. By using blockchain technology, the system's data security is strengthened even more, resulting in a strong, impenetrable architecture. Thorough testing has proven the system's resilience against a range of assaults based on trust models, proving its efficiency in protecting vehicle privacy. The outcomes of simulation demonstrate the practicality of the suggested method in actual VANET circumstances, pointing to the possibility of a new era in safe and private ITC systems.

Keywords:

Vehicular Ad-Hoc Networks (VANETS), Conditional Privacy-Preserving Authentication (CPPA).

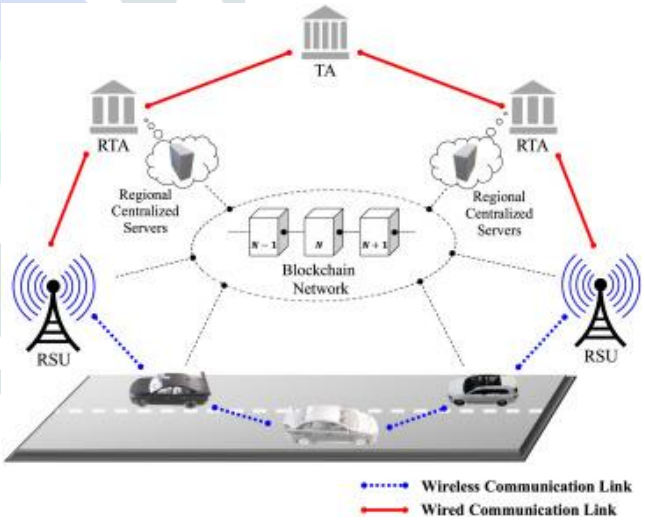


Figure.1. VANETs Architecture

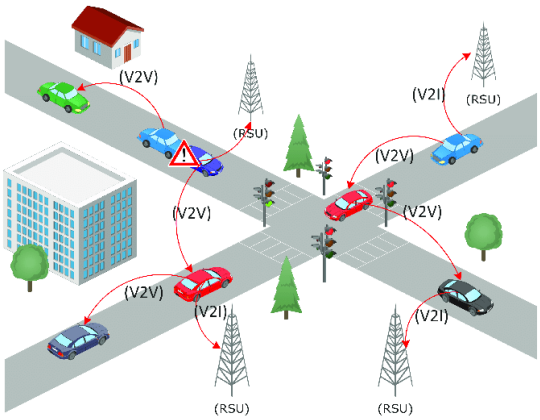
1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs), which promise to bring about dramatic improvements in traffic management, road safety, and transportation efficiency, have brought in a new era of greater connection and data interchange between cars and roadside infrastructure. But in order to safeguard the private and sensitive data being sent across these networks, strong security and privacy

measures are required. An inventive remedy has emerged to deal with these issues: The Effective Conditional Privacy-preserving Blockchain Technology

1.1 VEHICULAR AD-HOC NETWORKS (VANETS)

Modern transportation systems are leading the way in innovation thanks to Vehicular Ad-hoc Networks (VANETs), which combine wireless networking and vehicular communication. These networks are made expressly to allow cars to easily connect with roadside infrastructure and one another, forming a dynamic, ad hoc network while traveling. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication are key components of VANETs, which revolutionize vehicle-to-vehicle interaction on the road. These networks, which are outfitted with Roadside Units (RSUs) and On-board Units (OBUs), provide real-time information transmission that improves traffic management, road safety, and the driving experience overall. With our increasing reliance on smart technologies, VANETs play a pivotal



role in the development of intelligent transportation systems, offering enhanced efficiency and establishing the foundation for a safer and more connected road ahead. Block chain is a game-changing technology that has completely changed how data management and digital transactions operate. Fundamentally, a block chain is an unchangeable, decentralized ledger that securely and openly documents transactions made over a network of computers.

Figure.2. Overview of message Transmission using VANETs

1.2 CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION (CPPA)

Conditional Preservation of Privacy A novel approach to safe digital interactions is authentication (CPPA), especially when it comes to settings where privacy is a concern. In a time when safeguarding personal information is crucial, CPPA presents a novel method of authentication that puts user privacy first. CPPA modifies authentication depending on predetermined conditions, in contrast to traditional authentication approaches that frequently demand the revelation of sensitive information. This implies that, barring specific circumstances, consumers can access services and systems without jeopardizing their privacy. When it comes to conditional access to important documents, online platforms, or financial transactions, CPPA makes sure that authentication only takes place when all the right circumstances come together. Through the use of privacy-preserving protocols and cryptographic approaches, CPPA strengthens digital security while simultaneously giving users a greater sense of control and privacy when navigating the complex terrain of today's linked digital world.

2. LITERATURE SURVEY

[1] Because of the proliferation of cars and advances in wireless communication technology, Lu Wei and colleagues discuss in their study the growing significance of Vehicular Ad Hoc Networks (VANETs) in improving driving ease and traffic safety. Considering the vulnerability and security needs of VANETs, they determine that a Conditional Privacy-Preserving Authentication (CPPA) method is necessary. Not updating system secret key (SSK) updates stored in tamper-proof devices increases the possibility of SSK breaches, and traditional CPPA methods suffer from inadequately low communication/storage overhead for ultra-low transmission delay requirements of traffic emergency messages. To address these issues, the authors propose a CPPA signature scheme based on elliptic curve cryptography, ensuring message recovery and reduced communication overhead. They also introduce an SSK updating algorithm using Shamir's secret sharing and secure.

[2] An energy-efficient data forwarding system (EDFS) is introduced by Dapeng Wu et al. in their research with the goal of tackling important issues in Wireless Body Area Networks (WBANs), especially with regard to healthcare applications.

Because body sensors in these networks have limited energy resources, effective energy management is essential to preventing performance problems like latency and declining energy efficiency. In order to minimise the amount of physiological data supplied, EDFS uses compressed sensing. It also optimises the choice of relay sensors by taking into account variables like the relevance of the sensor, sampling frequency, and remaining energy levels. This method successfully adjusts to changing WBAN topologies while improving energy economy and network dependability.WBANs, a specialized subset of Wireless Sensor Networks, have garnered significant attention due to their capacity to collect diverse physiological data from wearable or implantable sensors, encompassing parameters like temperature, pulse, blood oxygen levels, blood pressure, electrocardiogram (ECG), and electroencephalogram, making them invaluable in the fields of biochemistry and healthcare.

[3] Duan and colleagues underscore the crucial function of Vehicular Ad Hoc Networks (VANETs) in the autonomous car sector, underscoring the growing security risks that coincide with progressions in VANET technology. They pinpoint weaknesses in the three-factor (3F) authentication strategy developed by Xu et al., which exposes it to the possibility of dishonest Roadside Units (RSUs) gaining access to the system without authorization and starting illicit sessions with On-Board Units (OBUs). In response, Duan et al. provide a unique 3F authentication system dubbed TFPPASV, which is intended to protect user privacy and foil RSU efforts to circumvent the TA. Their scheme is tailored to meet the security and performance requirements of VANETs and is subjected to rigorous formal security analysis using BAN-Logic, alongside informal discussions of its security features. Additionally, the authors compare TFPPASV's security and performance against other recent schemes. As VANETs gain popularity for their potential to enhance road safety and enable autonomous vehicles, this research underscores the need for robust security measures within this dynamic network structure, crucial for the future of transportation systems.

[4] With real-time traffic information sharing among cars, Chao Lin et al.'s solution addresses the security and privacy issues in vehicular ad hoc networks (VANETs), which have the potential to improve driver safety and traffic management efficiency. Especially with regard to VANET implementation, they draw attention to the shortcomings of the current conditional privacy-preserving authentication (CPPA) methods. The authors address these problems by putting forth a brand-new block chain-based CPPA (BCPPA) protocol that uses Etheruem as a public block chain to enable safe communication in VANETs.This innovative solution incorporates a key derivation algorithm, reducing the burden of storing numerous private keys for participating vehicles. To enhance verification efficiency, their BCPPA supports batch verification with modified ECDSA or alternative PKI-based signatures. Additionally, the authors outline the security requirements met by their protocol and demonstrate its feasibility through implementation on the Etheruem's test network.

[5] By addressing the shortcomings of current identity-based vehicular communication protocols, Jing Zhang et al. have developed a novel system that improves security and privacy in Vehicular Ad-hoc Networks (VANETs). In contrast to traditional techniques that depend on tamper-proof devices (TPDs), this new protocol makes use of the Chinese remainder theorem (CRT) to provide conditional privacy-preserving authentication without requiring master keys to be pre-loaded on TPDs in cars. This dynamic CRT-based approach facilitates the generation and dissemination of group keys by trusted authorities (TAs), mitigating side-channel attacks and bolstering overall system security. Importantly, it circumvents resource-intensive operations like bilinear pairing and map-to-point hashing during authentication, resulting in faster verification, even with an increasing number of signatures. Rigorous security analysis supports its resilience under the random oracle model, while performance analysis highlights its efficiency in reducing computational and communication overheads.

3. RELATED WORK

Traffic management may be streamlined and driver safety can be improved with the use of Vehicle Ad-hoc Networks (VANETs). In order to achieve the optimal balance between traceability, anonymity, and key/certificate management within VANETs, block chain-based conditional privacy-preserving authentication (BCPPA) is recommended. The existing procedures for BCPPA assist mitigate these security and privacy concerns by dramatically raising the cost of verification and traceability. The high mobility, low latency, and real-time performance requirements of VANETs are thus not met by current systems. Our proposal includes three new system building blocks: key derivation (KeyDer), smart

contracts, and signatures of knowledge (SoK). The more effective BCPPA technique that we create next is known as EBCPA. Message authentication, conditional privacy protection, and other pertinent criteria are among the first things we demonstrate that EBCPA can satisfy. prior to highlighting its advantages (resilience to frequent attacks, etc.). Furthermore, the EBCPA is implemented on the Hyper Ledger test network, the Rinkeby test network hosted online by Etheruem, and the VANET simulation environment (utilising VanetMobiSim and NS-2). Finally, to estimate its computational cost and communication overhead, we compare it to other BCPPA protocols that strive for similar goals.

4. METHODOLOGY

We suggest the Identity-Based Online/Offline Digital Signature (IBOOS) technique for secure data transmission in Cluster-based Wireless Sensor Networks (CWSN) to improve the performance of Wireless Sensor Networks (WSNs). In order to accomplish energy efficiency, we provide two new Secure and Efficient Data Transmission (SET) protocols: an improved CP-ABE method based on Diffie-Hellman cryptography and IBOOS, which expands upon the Identity-Based Digital Signature (IBS) technique. With these enhancements, the architecture becomes more streamlined, trusted authorities are involved less, and there is less communication overhead between them and Virtual Controllers (VCs). We create a central controller that houses the content server, RSU (ROAD SIDE UNIT), and vehicle information. This enables the development of many control servers with RSUs, each of which displays the content server IDs that are accessible in that RSU. Details about vehicle nodes are shown in the RSU interface, and RSUs are able to establish connections with the content server as needed. Furthermore, when the closest RSU is reachable, data replication within the car is made easier, which maximises data management in this situation.

According to the diagram showed, registering a car utilizing block chain technology is how it works. The Registration Authority (RTA) is where the procedure begins. This might be a government department or another company in charge of auto registration. The owner of the car applies for registration with the RTA. Details on the car, like the manufacturer, model, year, and VIN number, are included in this request. For the car, the RTA creates a key pair. A public key and a private key make up this key pair. While the private key is used to sign transactions, the public key is used to confirm the identity of the car. The vehicle's registration certificate is created by the RTA. This certificate is kept on a distributed, hard-to-tamper-with ledger called a block chain. After that, the car belongs to the owner. The registration certificate on the block chain can be updated by the new owner when the car is transferred or sold.

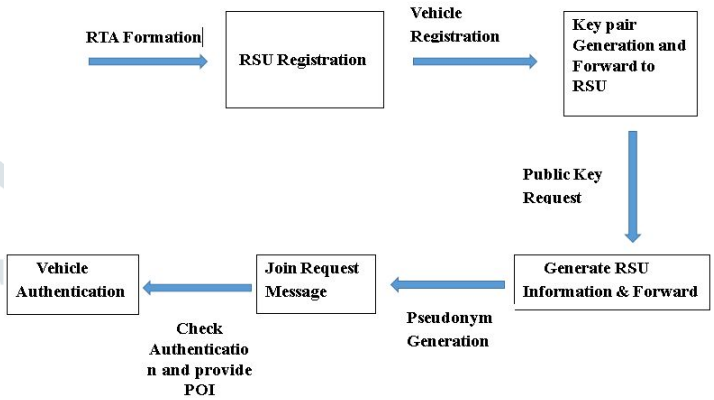


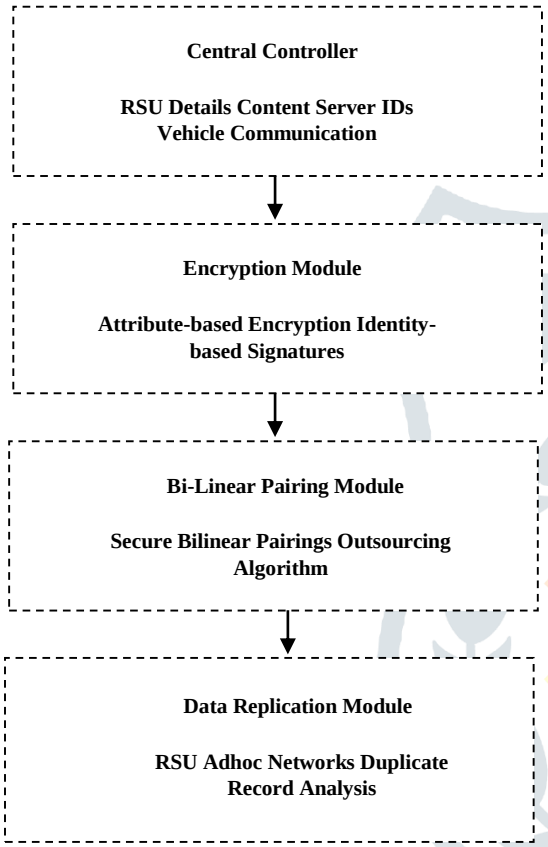
Figure.3. Block Diagram for Wireless Sensor Network

4.1 ENCRYPTION MODULE

Three crucial algorithms are involved in the proposed lightweight CP-ABE (Chipertext-Policy Attribute-Based Encryption) approach for mobile cloud-assisted cyber-physical systems. Distributing public parameters and safely preserving a master secret key for the system are the responsibilities of the first algorithm. By using the public parameters, input data, and access policy, the second algorithm—encryption—creates cypher text that is then sent to the cloud. The decryption algorithm, which ensures that only users whose characteristics meet the access policy may successfully decode the cypher text, is ultimately in charge of extracting the data from the cypher text using the master secret key and a set of attributes.

4.2 CENTRAL CONTROLLER SERVER

The central controller module acts as the main hub for controlling RSU information, content server IDs that are available, and enabling RSU-to-RSU communication with nearby cars. This module allows users to access and generate location IDs and RSU IDs within the content server. It also manages data replication in vehicles as part of the server's operation. Network administrators



can write SDN programmes for configuring, administering, securing, and optimising network resources since software-defined networks (SDNs) allow for programmable setup.

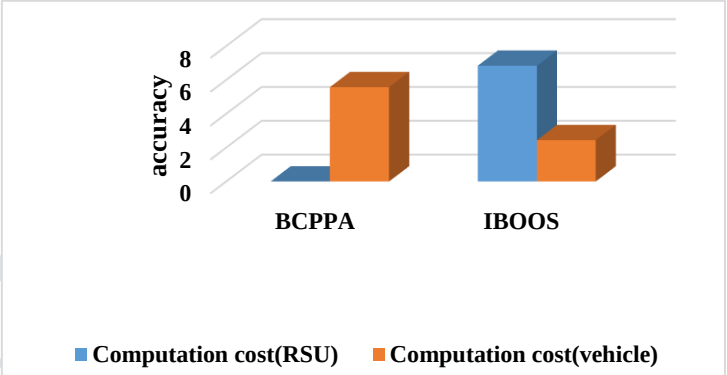
Figure.4. Flow Diagram for Wireless Sensor Network

4.3 BI LINEAR PARING MODULE

In order to reduce the computational overhead of bilinear pairings in pairing-based cryptography protocols, this research presents a novel strategy. We offer a safe and effective outsourcing technique that may be used in the two untrusted programme model. One salient characteristic of our method that sets it apart from current state-of-the-art solutions is that it spares the outsourcer from resource-intensive operations like exponentiations or point multiplications. Additionally, we use this method as a key subroutine in our effort to allow identity-based encryptions and signatures that are safe even when outsourced.

4.4 DATA REPLICATION MODULE

In this module, data replication is made possible by the increased accuracy of the RSUs (Roadside Units) in the vehicle ad-hoc



network. Each RSU has an ad-hoc model that it uses specifically to find and analyse duplicate information. In order to initiate the data replication module, this step entails finding matching records with other RSUs. Every RSU unit controls its own car ad hoc network, and the Database Replication module is used to import data from databases that already exist, even if such databases include complex mappings between numerous tables joins.

5. RESULT ANALYSIS

The accuracy of the suggested method is significantly higher than that of the current system. The accuracy of the new algorithm is 88%, which is a significant improvement above the 80% accuracy of the previous approach. This significant improvement in accuracy highlights how well the suggested solution works to address the problems found and enhance the overall functionality of Wireless Sensor Networks. The improvements show the potential of the suggested approach in safe and energy-efficient data transmission within Cluster-based Wireless Sensor Networks. Specifically, the implementation of the Secure and Efficient Data Transmission (SET) protocols and the Identity-Based Online/Offline Digital Signature (IBOOS) algorithm contribute to

Figure.5. Comparison Graph of BCPPA and IBOOS

the superior performance.

Scheme	BCPPA	IBOOS
RSU's Computation cost	13.5175 ms	6.8364
Vehicle Computation cost	5.5696	2.4415

Table.1. Comparison Table of BCPPA and IBOOS

6. CONCLUSION

In order to establish an area request, a querying vehicle sends a request to a nearby Roadside Unit (RSU) using a new block chain-based area security trust model outlined in this work. To establish anonymous secure zones, the RSU must coordinate with other cars to form a group. The query results are then returned to the vehicle that initiated the inquiry. By preventing direct contact between cars through the use of certificates as aliases, the system improves security and privacy while lowering the possibility of security breaches. The use of anonymous cover regions also offers defence against LSPs, or location service providers. The method under consideration utilises a consensus process for block chain maintenance called thermal reactor, which offers advantages over PoX in terms of computing efficiency and resource usage. Finally, a trust management technique is presented in the study and confirmed using experiments. While general trust models often incorporate trust incentive and token incentive models, this paper focuses on trust incentive and does not delve into token incentives. Future research will explore combining both incentive models to establish a more comprehensive trust model.

7.FUTURE WORK

Enhancing IBOOS and SET protocol performance: Both IBOOS and SET protocols are still in the development stage, therefore performance can still be improved. For instance, there is room for improvement in the efficiency of data encryption and decryption, message signing, and message verification. Minimizing the overhead associated with IBOOS and the SET protocols: Certain calculation and communication overhead is necessary for IBOOS and the SET protocols. This overhead could be decreased by creating protocols and algorithms that are more effective.

8. REFERENCE

1. Pokhrel S.R., Choi J., "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets", "IEEE Trans. Commun", Vol. 68, no. 8, pp. 4734-4746, Aug. 2020.

2. Baza M., Nabil M., Lasla N., Fidan K., Mahmoud., Abdallah M., "An energy-productive information sending technique for heterogeneous wbans", "In Proc. IEEE Far off Commun. Netw. Conf. (WCNC)", pp:1-7 April 2019.

3. Shrestha R., Nam S.Y., Bajracharya R., Kim S., "A three-factor security safeguarding validation plot for vanet", "Contraptions", Vol. 9, no. 9, p. 1338, Aug. 2020.

4. Jiang X., Tune F.R., Leung V.C.M., "A blockchain-based restrictive protection safeguarding validation convention for vehicular impromptu organizations", "IEEE Web Things J., early access", doi: 10.1109/JIOT.2020.3026354, Sep. 2020

5. Ayvaz S and Cetin S.C., "dad crt chinese remaining portion hypothesis based contingent protection safeguarding verification plot in vehicular impromptu organizations", "Int. J. Intell. Syst. Automate", Vol. 7, no. 2, pp. 72-87, Apr. 2019.

6. Guo R., Gao S., Zheng D., Jing C., and Wang L. "An accessible authentication method for blockchain that is traceable and protects privacy in VANETs", "IEEE Access", Vol:11, pp:7716–7726,2019.

7. Zeadally S., Feng Q., He D., and Liang K., "BPAS: Vehicle Ad Hoc Network Privacy-Preserving Authentication System Assisted by Blockchain", "IEEE Transactions on Industrial Informatics", pp: 4146-4155,2020.

8. Cui., Zhang., Zhong., and Liu., "Comprehensive conditional privacy protection authentication system for safe car networks in a multi-cloud setting",2020.

9. Zheng Z., Zhang Y., and Dai H., "A survey on blockchain and the internet of things". "IEEE Journal of Internet of Things"., 6(5), pp:8076–8094,2020.

10. Xu Jin H., Xu J., Liang W., and Li K., "An Internet of Vehicles key agreement protocol and authentication system based on blockchain for roadside units", "Journal of Parallel and Distributed Computing". pp:29–39, 2020.

11. M. Wellens, B. Westphal and P. Mahonen, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios", Proceedings of the 65th IEEE Vehicular Technology Conference (VTC007), pp. 1167-1171,2020.

12. Cottingham D., Wassell I and Harle R, "Performance of IEEE 802.11 a in vehicular contexts", IEEE Vehicular Technology Conference, pp. 854-858, 2007.

13.Wellens M., Westphal M and Mahonen P, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios", Proceedings of the 65th IEEE Vehicular Technology Conference (VTC007), pp. 1167-1171.

14.Jaballah M, Conti M and Lal C, "Security and Design Requirements for Software-defined VANETs", Computer Networks, vol. 169, March 2020.

15. Al-shareeda M., Anbar M., Manickam S and Hasbullah I H., "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network", Symmetry, vol. 12, October 2020.

16.Ramabadran R., Afanasyev P., Malone D., Leeser D., McCarthy D., Brien B O., et al., "A Novel Physical Layer Authentication with PAPR Reduction based on Channel and Hardware Frequency Responses", IEEE Transactions on Circuitsts and Systems Vol. 67, no. 2, pp. 526-539, February 2020.

17. Bottarelli M., Karadimas P., Epiphaniou P, Kbaier D., Ismail B and Maple B., "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 70, no. 3, pp. 2310-2321, March 2021.

18. Li J., Choo KR., Zhang W., Kumarid S., Rodrigues J., Khan MK., Hogrefe D., Efficient EPA-CPPA: "An. Provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks". Veh Commun 2018;240.

19 Sutrala AK., Bagga P., Das AK., Kumar N., Rodrigues JJPC., Lorenz P. "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment". IEEE Trans Veh Technol 2020;69(5):5535–48.

20 Vijayakumar P., Azees M., Kozlov SA., Rodrigues JJPC. "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs". " IEEE Trans Intell Transp Sys".2020.