IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Secure Vehicular Ad Hoc Network Communication using BlockChain

R. Arunachalam[1], Rajeswari. A[2], Serafin. J[3], Subathra. R[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India
r.arunachala@gmail.com and rajenthiransubathrasr@gmail.com

Abstract: *The vehicular social networks supports diverse kinds of services such as traffic management, road safety, and sharing data. Among these, secure data transmission has turned to be a spotlight. Ciphertext- policy attribute- based encryption may be adopted for data sharing. In traditional schemes, access policy is stored and granted by the cloud, which lacks credibility. To end this, we present a Blockchain Based Multi-Domain Vehicular Authentication scheme, in a which privacy-preserving authentication method is proposed to guarantee the Security.*

Keywords: Vehicular Ad Hoc Network(VANET); Communication BlockChain; SHA-256 algorithm; Authentication; Road Condition Report

REFERENCES

[1]. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[2]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 2,pp. 559–573, Feb 2010.

[3]. F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, Dec 2015.

[4]. "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages,"IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240,March 2016.

[5]. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, March 2017.

[6]. L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, March 2011.

[7]. Y. Liu, J. Ling, Q. Wu, and B. Qin, "Scalable privacy-enhanced traffic monitoring in vehicular ad hoc networks," Soft Computing, vol. 20, no. 8, pp. 3335–3346, Aug 2016.

[8]. R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud based vehicular networks with efficient resource management,"IEEE Network, vol. 27, no. 5, pp. 48–55, September 2013.

[9]. J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, December 2015.

[10]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp.50–58, Apr. 2010.

[11]. C. Gentry, "Fully homomorphic encryption using ideal lattices,"in Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, ser. STOC'09. New York, NY, USA: ACM, 2009, pp. 169–178.

[12]. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and ` J. A. Manjon, "Contributory broadcast encryption with efficient ´encryption and short ciphertexts," IEEE Transactions on Computers, vol. 65, no. 2, pp. 466–479,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Feb 2016.

[13]. L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 601–610, April 2017.

[14]. V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," Computers & Security, vol. 60, pp. 193–205, 2016.

[15]. A. Malhi and S. Batra, "Privacy-preserving authentication framework using bloom filter for secure vehicular communications,"International Journal of Information Security, vol. 15, no. 4, pp. 433–453, Aug 2016.

[16]. Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," IEEE Transactions on Industrial Informatics, pp. 1–1, 2018.

[17]. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," IEEE Computer, vol. 45, no. 1, pp. 39–45, Jan 2012.

[18]. B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in the cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, Dec 2014.

[19]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores,"in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007,pp. 598–609.

[20]. A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.

[21]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology–ASIACRYPT 2009, M. Matsui, Ed. Springer Berlin Heidelberg, 2009, pp. 319–33