IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Network Security

Likhita K M[1], Mr. Nagesh U B[2], Finny Paul[3], Keerthana G[4], Gary Richards[5]
Faculty, Department of Information Science and Engineering[2]
Students, Department of Information Science and Engineering[1,3,4,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *Today, nations all over the world are actively supporting the advancement of intelligent agriculture. They must individually grow unique plants that are matched to the area for farming, and this information is crucial and delicate. This is why information-driven, intelligent agriculture needs network security protection to guarantee data privacy and integrity. This study suggests using dark web technology to protect the privacy of servers and blockchains. In intelligent agriculture, packet transfer frequency will be monitored to guard against distributed denial-of-service (DDOS) assaults. The system's key features are: (1) an identity authentication method; (2) secure information transfer; (3) the creation of private blockchains; (4) a quicker, more effective system for blockchain information authentication; and (5) resilience to DDOS attacks. The proposed system can protect network security for IoT devices as well as servers by utilising dark web technology, which can reduce the risk of DDOS attack damage by preventing the visibility of blockchains and server ID addresses. Results from the experiments show that the suggested scheme's use of lightweight encryption does, in fact, speed up authentication while simultaneously meeting network security criteria.*

Keywords: Network Security

REFERENCES

[1]. Kaufman, Perlman and Speciner, Network Security: Private Communications in a Public World, second edition (Prentice Hall, 2003).
[2]. BS 7799-2 (2002) Information Security Management Systems – Specification with Guidance for Use , British Standards Institution.
[3]. Ellis, J. and Speed, T. (2001) The Internet Security Guidebook, Academic Press. 4. Cheswick and Bellovin, Firewalls and Internet Security, 1/e (Addison-Wesley, 1994; free online for personal use). Second edition with Rubin (Feb.2003).
[4]. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus.Rev. 2008, 10, 21260.
[5]. Aggarwal,S.;Chaudhary,R.;Aujla,G.S.;Kumar,N.;Choo,K.K.R.;Zomaya,A.Y.Blockchainforsmartcommunities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019, 144, 13–48. [CrossRef]
[6]. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174. [CrossRef]
[7]. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A machine learning approach for blockchain-based smart home networks security. IEEE Netw. 2020, 35, 223–229. [CrossRef]
[8]. Zhou, Z.; Wang, B.; Dong, M.; Ota, K. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Trans. Syst. Man Cybern. Syst. 2019, 50, 43–57. [CrossRef]
[9]. Wu, J.; Dong, M.; Ota, K.; Li, J.; Yang, W. Application-aware consensus management for software-defined intelligent blockchain in IoT. IEEE Netw. 2020, 34, 69–75. [CrossRef]
[10]. A. Almeida, D. Doneda, and M. Monteiro, "Governance challenges for the internet of things," IEEE Internet Comput., vol. 19, no. 4, pp. 56–59, 2015.
[11]. K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet of things: Research challenges and opportunities, "IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567–3569, 2018.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

[12]. T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency internet of things," IEEE Trans. Mobile Comput., vol. 17, no. 1, pp. 72–84, 2018.

[13]. Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," IEEE Access, vol. 25, no. 6, pp. 12–18, 2018.

[14]. J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2526–2536, 2018.

[15]. J.Granjal,E.Monteiro,andJ.S.Silva,"Securityfortheinternetofthings: A survey of existing protocols and open research issues," IEEE Commun. Surveys Tut., vol. 17, no. 3, pp. 1294–1312, 2015.

[16]. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacyissuesininternet-of-things,"IEEEInternetThingsJ.,vol.4,no.5, pp. 1250–1258, 2017.