An Analytical Approach for Optimization of Block Chain Security for Internet of Things

Mr. Harshal Nikam[1] and Dr. R. M. Deshmukh[2]
Professor and Head, Department of Electronics and Telecommunication[2]
Dr. Rajendra Gode Institute of Technology & Research, Amravati, Maharashtra, India
harshalnkm@gmail.com[1] and ravindra.dshmkh@gmail.com[2]

Abstract: *The number of smart devices or IOT devices either it may be a smart phone, smart home, tablet or any wearable devices are connected to internet are increasing day by day. Due to this numerous number of security threats are searching for loopholes that are ready to exploit any type of network. Security threats have become critical challenges against the backdrop of recent rapid raising advancements of IOT technology that demands continuous and responsive action. As a demanding technology Internet of Things (IoT) needs best information security features for effective IOT smart city and technological activity development. In this paper an Implementation of IoT system using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention is presented. The block chain distributed behavior makes this system more immune and robust for a single failure. A Zero-Knowledge proof technique is applied for preventing the third party from checking user's original information. Integrity validation test and avalanche effect technique is processed for block chain, MD5 and SHA-256 which results the proposed block chain technology has better security.*

Keywords: Block Chain, Internet of Things, Intrusion Detection, Malicious Attack, Security Threats

References

[1]. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. 2017, 112, 237–262

[2]. Rajneesh Kumar, Shekhar Verma, G S Tomar, "Thwarting Address Resolution Protocol Poisoning using Man In The Middle Attack in WLAN", International Journal of Reliable Information and Assurance Vol.1, No.1, pp.8-19, 2013

[3]. Diana Yacchirema, Carlos Palau, "Interworking of Onem2M-Based IoT Systems and Heterogeneous IoT Devices", 2020 XLVI Latin American Computing Conference (CLEI), Year: 2020

[4]. S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities," IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60–70, July 2016.

[5]. Jianming Liu, Ziyan Zhao, Jerry Ji, Miaolong Hu, "Research and application of wireless sensor network technology in power transmission and distribution system", Intelligent and Converged Networks, Volume: 1, Issue: 2 , Year: 2020

[6]. Yang, H.K., Cha, H.J. and Song, YJ, 2019. Secure identifier management based on blockchain technology in NDN environment. IEEE Access, 7, pp.6262-6268.

[7]. A. Pentland and E. Castello Ferrer, "Blockchain: A New Framework for Robotic Swarm Systems," Media Lab Research MIT; www.media.mit.edu/projects/blockchain-a-new-framework-for-swarm-robotic -systems/overview.

[8]. N. De, "Hacks, Scams, and Attacks: Blockchain's 2017 Disasters," 29 Dec. 2017, coindesk; www.coindesk .com/hacks-scams-attacks -blockchains-biggest-2017-disasters.

[9]. Basic Attention Token (BAT): Blockchain Based Digital Advertising, white paper, Brave Software, 13 Mar. 2018; www.basicattentiontoken.org /BasicAttentionTokenWhitePaper - 4.pdf.

[10]. N. Lomas, "What Do AI and Blockchain Mean for the Rule of Law?," 12 May 2018, Techcrunch, https:// techcrunch.com/2018/05/12/what -do-ai-and-blockchain-mean-for -the- rule-of-law.

[11]. L. Fan and H.-S. Zhou, "A Scalable Proof-of-Stake Blockchain in the Open Setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake," 2018; https:// eprint.iacr.org/2017/656.pdf.

DOI: 10.48175/568

[12]. J.I. Wong, “Every Cryptocurrency’s Nightmare Scenario is Happening to Bitcoin Gold,” 24 May 2018, Quartz; https://qz.com/1287701/bitcoin -golds-51-attack-is-every -cryptocurrecnys- nightmare -scenario.

[13]. A. Hern, “AI Used to Face-swap Hollywood Starts into Pornography Films,” 25. Jan 2018, The Guardian; www.theguardian.com/technology /2018/jan/25/ai-face-swap -pornography-emma- watson-scarlett -johansson-taylor-swift-daisy-ridley -sophie-turner-maisie-williams.

[14]. G. Wood, “Web3 Foundation,” 2017; https://web3.foundation.

[15]. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, “A blockchain-based architecture for collaborative ddos mitigation with smart contracts,” in IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Cham, 2017, pp. 16–29.

[16]. A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, “Systas: Density- based algorithm for clusters discovery in wireless networks,” in 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2015, pp. 2126–2131