applied sciences

MDPI

Review

Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review

Jamil Asim [1,2,*], Adnan Shahid Khan [1,*], Rashad Mahmood Saqib [1,3], Johari Abdullah [1], Zeeshan Ahmad [1,4], Shehla Honey [5], Shehroz Afzal [1,6], Malak S. Alqahtani [7] and Mohamed Abbas [4,8]

1 Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia; rsaqib@kau.edu.sa (R.M.S.); ajohari@unimas.my (J.A.); zayshan@kku.edu.sa (Z.A.); shehrozafzal347@gmail.com (S.A.)
2 Department of Criminology, University of Okara, Okara 56300, Pakistan
3 Faculty of Applied Studies, King Abdul Aziz University, Jeddah 21589, Saudi Arabia
4 Department of Electrical Engineering, College of Engineering, King Khalid University, Abha 61421, Saudi Arabia; mabas@kku.edu.sa
5 Department of Physics, University of Okara, Okara 56300, Pakistan; shehlahoney@uo.edu.pk
6 Department of Computer Science, University of Narowal, Narowal 51600, Pakistan
7 Faculty of Technology, The Gatway, De Montfort University, Leicester LE1 9BH, UK; qmalak46@gmail.com
8 Computers and Communications Department, College of Engineering, Delta University for Science and Technology, Gamasa 35712, Egypt
* Correspondence: jamil.asim@uo.edu.pk (J.A.); skadnan@unimas.my (A.S.K.)

Abstract: There are continued advances in the internet and communication fields regarding the deployment of 5G-based applications. It is expected that by 2030, 6G applications will emerge as a continued evolution of the mobile network. Blockchain technology is one of the leading supporting technologies predicted to provide a secure and unique network to 6G-enabled devices, transactions, and applications. It is anticipated that the 6G mobile networks will be virtualized, have cloud-based systems, and aim to be the foundation for the Internet of Everything. However, along with the development of communication technologies, threats from malicious parties have become more sophisticated, making security a significant concern for the 6G era in the future. Despite enormous efforts by researchers to improve security and authentication protocols, systems still face novel intrusion and attacks. Recently, multifactor authentication techniques (MFA) have been deployed as potential solutions to attacks in blockchains. The 6G applications and the cellular network have specific vulnerabilities that need to be addressed using blockchain-based MFA technologies. The current paper is a systematic review that discusses the three technologies under consideration; then, several studies are reviewed that discuss MFA techniques in general and use blockchains as potential solutions to future security and authentication issues that may arise for 6G applications.

Keywords: 6G cellular network; blockchain technology; multifactor authentication technique; network security

Citation: Asim, J.; Khan, A.S.; Saqib, R.M.; Abdullah, J.; Ahmad, Z.; Honey, S.; Afzal, S.; Alqahtani, M.S.; Abbas, M. Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. *Appl. Sci.* **2022**, *12*, 3551. https://doi.org/10.3390/app12073551

Academic Editors: Howon Kim and Thi-Thu-Huong Le

Received: 13 March 2022
Accepted: 29 March 2022
Published: 31 March 2022

1. Introduction

Blockchain technology involves recording information that makes it hard to change, cheat, or hack the system [1,2]. An exciting aspect of blockchain is the application with authentication, which formulates a system with multiple layers of security and authentications [3]. Blockchain-based mechanisms solve authentication problems for distributed ledger technologies [4–6]. Still, a significant amount of work is required to assist with machine learning models to predict incoming attacks or security threats [7]. So, similarly, the 6G applications and cellular networks also have specific vulnerabilities, which need to be addressed through the application of blockchain-based multifactor authentication technologies [8]. As the former applications are mainly based on artificial intelligence Visible light communication (VLC) technology, both are significantly vulnerable when it