Blockchain-based multifactor authentication for future 6G cellular networks: a systematic review.

ASIM, J., KHAN, A.S., SAQIB, R.M., ABDULLAH, J., AHMAD, Z., HONEY, S., AFZAL, S., ALQAHTANI, M.S. and ABBAS, M.

2022

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

comes to encryption, malicious behavior, and data transmission, which can be considerably problematic [9,10].

Blockchain technology can establish a creditworthy ecosystem among different participants in a non-trustable distributed environment. For example, in cybersecurity, the use cases of the blockchain depend on different security parameters that are applied for authentication, identification, and authorization in organizations which have also become penetrable [11]. After introducing the cloud-based applications and other extensive cloud-based technologies, the challenges of authentication are enhancing, presenting various challenges and threats to individuals and organizations. Moreover, the threats related to authentication, identity management, and access control security in different environments and organizations also serve as challenges to various industries [11]. Communications between devices and things that are enabled to receive and process information due to embedded computing components, such as the Internet of vehicles or the Internet of Things, are significantly impacted by the challenges of authentication and security. As a result of these threats, different studies have proposed some access control technologies to address the extensive authentication and security issues faced by organizations, individuals, and industries [12,13].

Apart from the exchange of images, voices, and video-based information available in 5G cellular networks, the researchers are now focusing on the new dimensions of interactions that involve five senses of communication, including the ubiquitous instant communications, internet of skills, virtual or augmented reality, pervasive intelligence, wireless brain–computer interfaces, and holographic communications, leading towards the emergence of the distant environment [14,15]. The researchers are now analyzing and focusing on smart communication in different sectors, including autonomous driving, industry Internet, remote learning sector, health care sector, smart cities provided by 5G networks, and the secured transactions sector [16]. However, the smart cities connected to 5G networks have faced some limitations concerning the networks' reliability, security, and speed. This has increased the focus of researchers and practitioners on the 6G network developments as it promises to overcome the issues of latency, speed, and security associated with prior networks [17,18]. Various researchers and experts have envisioned the 6G wireless networks to provide data-intensive smart societies in the future, having a significant level of automation and seamless wireless network integration throughout the underwater area, to the ground, air, and space [19].

With significant enhancement and growth of the emerging multimedia applications and data traffic, the 6G wireless network is predicted to cater to 607 exabytes of data traffic by 2025 and, in 2030, around 5016 exabytes per month [13]. It is anticipated that the 6G mobile networks will be virtualized through cloud-based systems and is software-defined, intending to ubiquitously connect several heterogeneous devices like the Internet of everything, to enable a significant range of different network services. With this shift of the paradigm towards the 6G network, blockchain and the Internet of Things play a critical role in enabling the applications that connect the cyberspace of the communication world with the physical devices [20,21]. The future generation of wireless networks supports data-intensive and real-time applications that involve sustainable business models, network orchestration, agile management, spectrum sharing, network slicing, and several other vertical services, so the researchers and experts are increasingly focusing on these terms and systems now [11].

Based on the increasing trends towards the usage of blockchain-based multifactor authentication and a 6G cellular network, the objectives of the study are: (1) to explain and define the blockchain, Multi-factor Authentication, 6G, and the benefits blockchain integration of in 6G, (2) to explore current strategies for the use of blockchain-enabled MFA, and (3) to suggest how the integration of blockchain-enabled MFA would be beneficial for 6G. This study will be a significant addition to the existing literature on blockchain, multifactor authentication, and 6G networks, as it differs from other reviews available in the domain. The current study uses a systematic review style to collect, organize and

present information extracted from the reviewed articles published between 2015 and 2021; thus, the study provides more up-to-date and recent information.

The selected journal will be reviewed based on different aspects, including the studies' strengths, weaknesses, methodologies, data sets, and evaluation metrics. Furthermore, based on the review of the relevant articles and studies, this study provides details regarding the recent trends related to blockchain-based multifactor authentication and 6G cellular network strategies and integration. Based on these, the study includes the limitations and future indications. This study significantly contributes to explaining the multifactor authentication, blockchain and 6G-based phenomenon, strategies, integrations, and benefits and helping the users in decision-making processes regarding the adoption of the up-to-date systems of blockchain, multifactor authentication 6G mobile networks. Table 1 represents the comparison of the study with the other similar and relevant review articles. The table represents whether or not the study in comparison is a systematic study, blockchain-focused, MFA-focused, 6G-focused, and focused on future trends of these technologies.

Table 1. Comparison with other similar review articles (✓: Yes, ×: No).

Study	Year	Systematic Study	Blockchain Focused	MFA Focused	6G Focused	Future Trends
[9]	2021	✓	✓	×	✓	✓
[14]	2020	✓	✓	✓	✓	×
[13]	2021	✓	✓	✓	×	✓
[20]	2020	✓	✓	✓	✓	×
[22]	2020	✓	✓	×	✓	✓
This study	2022	✓	✓	✓	✓	✓

The rest of the paper is organized as follows: Section 2 details the research methodology used in this research. Section 3 discusses the 6G cellular concepts and security needs. Section 4 explains the Multifactor authentication schemes, followed by a blockchain discussion in Section 5. Section 6 provides details regarding recent studies that have listed some MFA techniques or applications of MFA to a blockchain. Section 7 details the observation based on this review study to highlight the current and future trends and the research challenges. Finally, Section 8 concludes this research study.

2. Methodology

The study has been conducted systematically in view of different research and experimental studies on the multifactor authentication techniques, preferably including the concepts of multifactor authentication, 6G, and blockchain. We focused on the published journal articles ranging from the year 2015 to the year 2021. A systematic approach is adopted for the review process, which is the type of methodology utilized and applied to identify, examine, and extract needful information from literature relevant to a specific research topic. The review has been done in two different phases. The first phase involves the identification of information resource that was the search engine and keywords that were utilized for the execution of the query. Whereas the second phase includes the application of specific criteria onto the initial generated list so that only the most relevant articles are shortlisted for the final list of the papers reviewed for the systematic literature review. Figure 1 depicts both phases of the review process adopted in this study.

We conducted comprehensive research in this review. In the first phase, the keywords and the search engine are identified for searching the articles. The researcher critically evaluated the research published in the English language between January 2015 and December 2021. The reason for focusing on these years is that the 6G technology research emerged in this era. For this study, "Scopus document search" and "Ebsco databases" are the chosen search engine because of their efficiency in searching through all authentic databases. The search keywords include "multifactor authentication in blockchains", "multifactor authentication in blockchains, and 6G cellular network". Once the search

query is executed, the initial list of the articles is obtained. Retrieval run on both databases resulted in 299 papers, 191 papers collected from Scopus, and 108 from Ebsco. At the end of the process of overviewing and removing duplicated articles or whose full text could not be retrieved, 124 articles were left of the initial research of 299, 71 papers were collected from Scopus and 53 from Ebsco. After this, the abstracts were reviewed before the complete screening of material. In this stage, a further 41 articles were dropped. The final set of 73 papers was included in the review; 57 were retrieved from Scopus and 16 from Ebsco. All the retrieved references from the various databases included in the study were then added to the software used in this study for reference management, i.e., Endnote Version 9.2. Table 2 shows the papers included in this review in each domain.

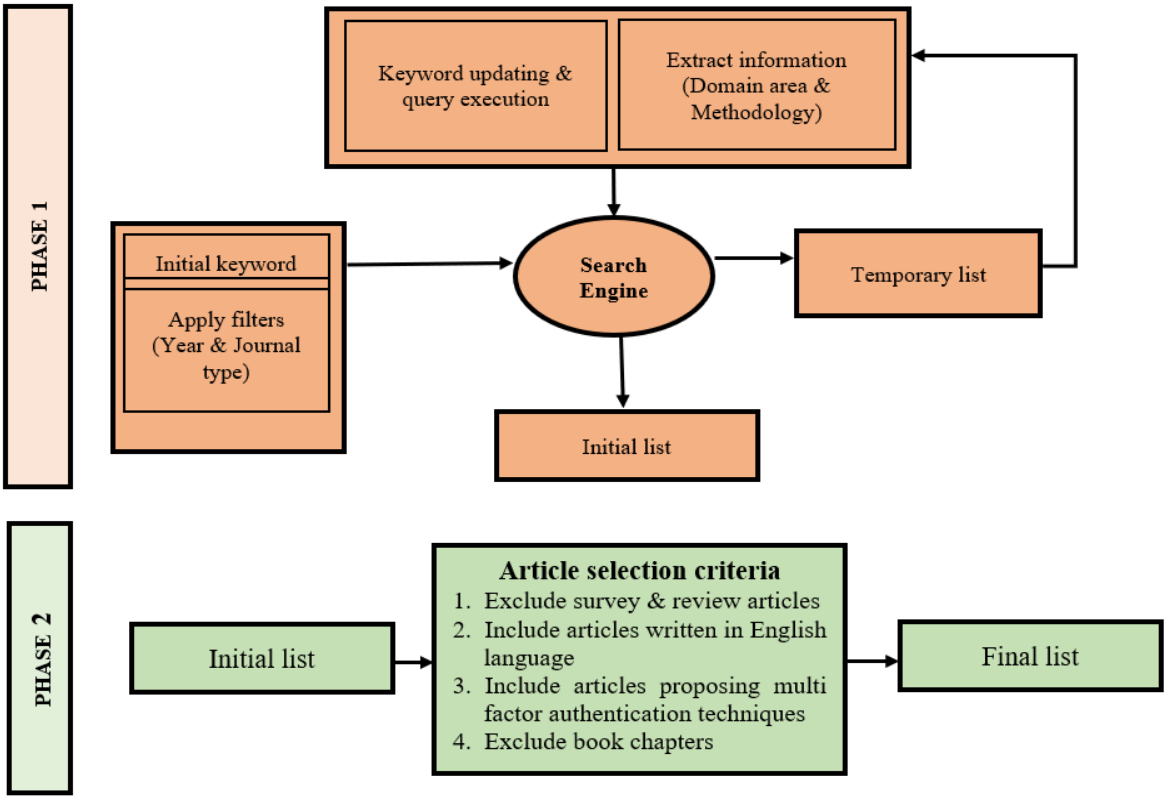

Figure 1. Research methodology (Phase 1 and Phase 2).

Table 2. Summary of included research papers.

Domain	Number of Papers
Networks (2G, 3G, 4G, 5G, 6G)	8
Blockchain	30
Multifactor Authentication	28
Data, Security, Reliability, or other issues	7

In the second phase, we analyzed the initial list. We then defined a specific criterion for obtaining the articles that are significantly relevant and more focused on the multifactor authentication in blockchains and 6G cellular network for the final systematic review. Book chapters and survey/review-based articles are excluded to select more focused articles for this study. Additionally, articles are included that propose some multifactor authentication techniques and are written in English.

3. 6G Cellular Network

3.1. Concept and Development

With the research community involved in discussing possibilities and opportunities that may be opened up with the materialization of 6G technology, most countries in the world are still caught up in the deployment of the 5G technology. However, it is hypothesized by most researchers that 5G and Beyond 5G (B5G) technologies, once fully deployed, will be capable of enabling the Internet of Everything (IoE) to truly take off [23,24], leading to justifying the massive demands for 6G. The sixth generation of wireless technology (6G) will focus on communication between connected machines, i.e., thing-to-thing connection instead of people-to-people links in 1G-4G and people-to-thing communication as in the focus of 5G, as represented in Figure 2.

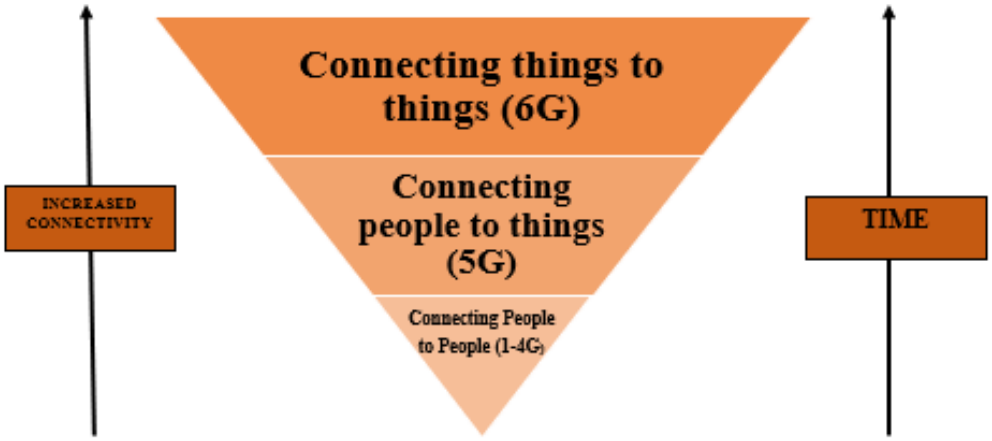

Figure 2. Evolution of Internet.

In the past, a new wireless communication standard emerged after around a decade, and given this trend, it is expected that we would be witnessing 6G around 2030 [25–27]. As more and more users are connecting to the internet and using a large number of devices connected to the Internet, big changes and challenges are coming up for internet research. The research communities are already looking towards solutions to the challenges posed by 5G mobile communication. It is expected that many of these challenges will be addressed by the time 6G materializes [20,28].

3.2. Security Needs

While 6G applications and communication technologies will be powerful and a revolution, there will be many specific vulnerabilities [20]. Communication, access control, malicious behavior, authentication, and encryption-related issues will be faced in these applications (see Figure 3 below). It can be seen in the figure that 6G will support autonomous systems powered by A.I. and ML, multi-sensory X.R. applications built upon molecular communication technology, the THz technology, and the quantum communication technology and distributed ledger technologies that will be mainly developed using blockchains, etc. A.I. technologies and multi-sensory X.R. applications will be susceptible to issues with malicious behavior, encryption, and communication due to heavy data transmissions; however, the blockchains and DLT will be relatively safe as they already implement techniques of multistep or multifactor authentication.

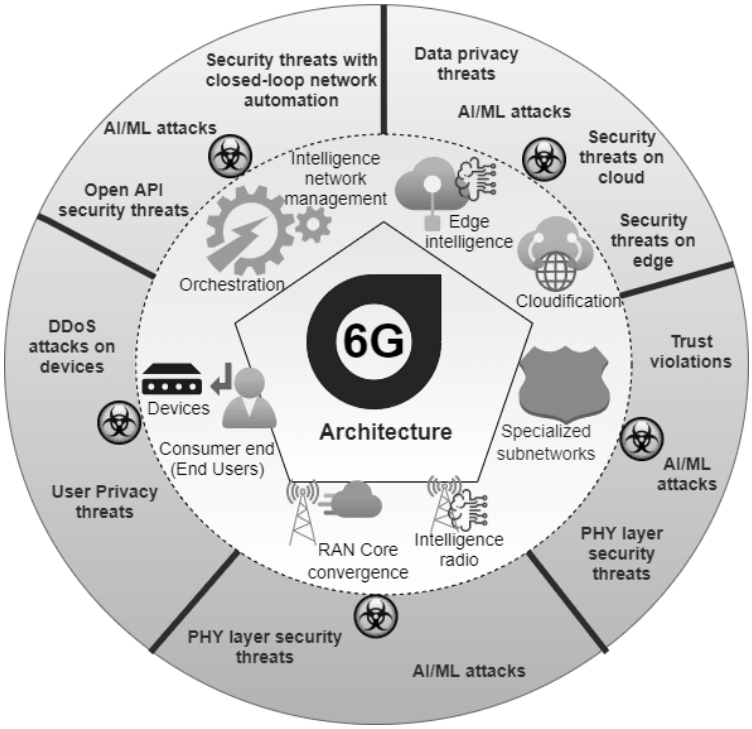

Figure 3. Security and Privacy issues in 6G networks.

4. Multifactor Authentication

4.1. Concept and the Main Goal

Multifactor authentication is a technology developed for security purposes and requires multiple kinds of authentication from multiple independent sources and through varying credentials to verify the user's identity [16,29]. The MFA is mainly developed for logins and transactional purposes [30,31]. The primary goal of the MFA is to design a layered defense that makes the accessibility of an unauthorized person to the device, location, network, and database difficult [32]. If one of the barriers or layers is accessed, the attacker, hacker, or simply the unauthorized person has to get through one or more security layers to completely breach the applications and systems through software and hardware. The main goal behind the development of multiple authentications was to increase the security and also to increase the integrity of the digitized transactions [33,34]. Figure 4 presents the basic framework for the architecture of the MFA system.

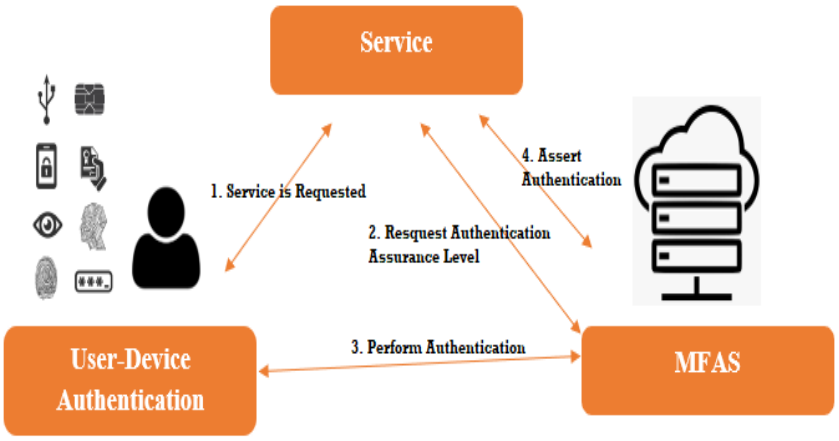

Figure 4. Basic Architecture of MFA system.

4.2. Use of MFA

MFA is a development that has been aimed at increasing the level of security of the authorized access to personal information, resources, and important data. In accordance with the Commission Implementing Regulation (E.U.) 2015/1502 [35], a secure and strong authentication process is based on at least two authorization factors. The MFA uses the shortcomings of the single and double authentication and the traditional I.D. and password mechanisms, and the developers use these to develop a more secure method. The main problem with less sturdy mechanisms of authentication is that the users become susceptible to hacking, security breaches by compromising the passwords and, in the case of financial transactions, costing large sums of money to the users [16]. Brute force attacks are also an actual hazard, as hackers and other bad actors can use the automated passwords, thereby cracking the safety protocols by trial and error until they arise on the correct sequence. However, some accounts and application developers enable locks after multiple incorrect password attempts, helping the organizations track and protect their users. Thus, one of the primary uses of the MFA is its characteristic of reducing the security risks [30,36–40]. There are different ways through which the MFA is enabled. Table 3 illustrates the methods through which MFA is enabled.

Table 3. Various Types of MFA and its Pros and Cons.

MFA Type	Process	Pros	Cons
Hardware OTP [37,38]	- A one-time code is generated using the cryptographic keys stored inside devices - This key is also accessed by the server, which generates a similar OTP to confirm the OTP against the values provided by the user. - Interfaces may include token representation of OTP on screen /device requiring user to enter PIN for accessing it.	- Easy to adopt - Gives the OTP - Available widely - Email signing and encryption - Customization possible.	- A Weak user experience, due to which the users are limited in the operation of tasks, which is not compatible with technological and lifestyle factors. - High costs for operation and maintenance. - Only works on compatible infrastructures.
Authenticator Applications [16,39]	- Different applications such as google authenticator and Microsoft authenticator. - These applications are mere versions of the authenticator applications and act as a version of the authenticator application which is used for multifactor authentication.	- Once set up in the designated devices, it can be used without internet access.	- Needs user to switch between the applications to authenticate the identity, user, and transaction losses with every software and device upgrade. - Requires a phone for application or usage. - Lack of support for businesses relying on third-party applications. - The capacity of malicious softwares to steal and impersonate the users.

Table 3. *Cont.*

MFA Type	Process	Pros	Cons
Soft Token Software Development Kits (SDKS) [15,16,39,40]	- It can be implanted into the devices that utilize cryptographic operations for verifying the user and device. - Generally, provides a smooth user experience, and therefore, there is not any need for switching applications or relying on a hardware device. - From the perspective of security, there are numerous advantages to the usage of the SDKs as they support advanced cryptography, e.g., digital signatures.	- Free of cost - Applications such as google authenticator, postal guard, a password reset can easily be found on app stores. - Does not require cellular signals for operating. - Accessibility and ease of usage.	- Framework does not allow batch imported by the administrators. - Only one application can be used. - User are required to constantly alternate or switch between the apps for authentication of the mobile phones. - Less support for business reliance on the it.
OTPS Based On SMS [29,36,41,42]	- A user-friendly method framework that does not require external explications for application installation. - Mobile devices that are capable of receiving text messages are usable for this kind of MFA.	- Mobile devices capable of receiving the SMS are safe for usage and these do not require smartphones explicitly for usage. - There is not additional hardware required for the delivery methods.	- Requires cellular connectivity. - Requires strong signals and battery life. - The OTP can be used by any person holding the device. - Codes sent through SMS are all susceptible to malware and hacking. - The OTPs and the message scans are all susceptible to phishing by the hackers.
Hardware Tokens [29,31,32,36,39]	- These are physical devices that can perform cryptographic operations such as digital signing and decryption. - These can be used for logging on to the P.C.s, systems, entering into the building.	- Smart cards, e.g., with higher level of security than other data storage devices. - Difficult to breach systems established via hard tokens. - Requires less connectivity to work. - Mostly tokens are operable without the Internet, so minimizes the susceptibility to online threats. - Presence of security keys embedded in the tokens increases the security.	- High costs of maintenance, operation, deployment, upgrade, and replacement. - Posses' similar issues in the user experience as the OTP hardware tokens. - The breaches can be more severe. Even though it is more difficult to steal or replicate a hard token.

4.3. Advantages of MFA Implementation

First, the primary benefit of MFA is the fact that it provides a superior level of security as it adds an extra layer of security to reduce access to sensitive data and protected systems [41–44]. Many employees in today's organizations work from their homes, leading to increased exposure to cyber threats and data breaches. MFA allows 99.9% of automated password breaks to be blocked [40,41,45–49]. MFA can also protect against credential and device theft as it ensures that a password alone cannot authenticate a login attempt [50–52]. Another advantage to MFA is that it is one of the easiest and least costly cybersecurity solutions. MFA is non-intrusive and does not cause downtime, so it is easy to use and implement [44,45,53,54]. It also allows for Single Sign-On (SSO) compatibility by providing options of a one-time password (OTP) so that an active login session is not exploited to unlock any additional accounts [55,56]. MFA also provides organizations with an opportunity to meet all the security-related regulatory requirements without extra effort [57].

5. Blockchain Technology

5.1. What Is Blockchain Technology?

Blockchain technology can be claimed to be the most-hyped innovation of the 21st century that was designed to support bitcoin but now powers many business applications and is hyped to be the leading technology for the support of 6G technologies [22,58,59]. Advancements in blockchains are still young and hold the promise of a bright future [60–62]. The blockchains can be defined as a digital ledger of transactions (DLT), a database that can store encrypted transaction data in chronological order and chain the data together in the form of blocks [63,64]. Blockchain is used to define a structure of data that can be described as an ordered arrangement of blocks, where each of the blocks contains a small list of transactions and each of the blocks is chained together [65–67]. Through these chains, each component of the data can be traced to its source; however, the blockchains cannot be altered, deleted, or replaced without invalidation of the hash chain [65]. Blockchain technology has extensive applications in payment systems and other digital financial or Fintech solutions. Thus, this technology requires strict authentication protocol for managing the safety of the users and transactions [15,32].

5.2. How does Blockchain Work?

This technology, therefore, enables safe transactions between individuals without the fear of government, bank, or other third-party software snooping and stealing the data [68,69]. Figure 5 maps out roughly how a blockchain works; first, an individual node in a peer network requests a transaction, which is then broadcasted to a P2P network of nodes that authenticates it by verification technique and combines it to other transactions to form an encrypted block of data which is added to an existing blockchain [70,71]. Blockchains can be considered, therefore, as a promising and revolutionary technology for future developments of applications in the 6G network era as it can help in reducing the risks, stamps out frauds, and brings multilayer transparency in any transactions between two nodes in a scalable way, opening up a myriad of application scope and uses.

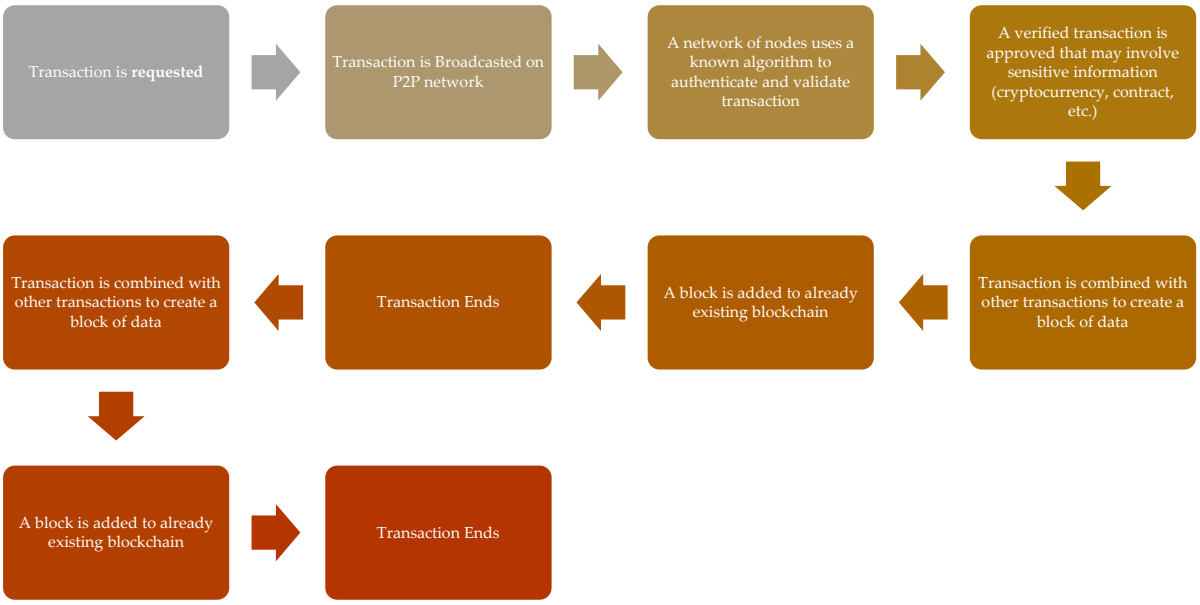

Figure 5. Blockchain Working.

5.3. Benefits of Blockchain

Blockchains are gaining rapid fame due to the importance of record-keeping and storage of transactions and their crucial status for various kinds of businesses [72–74]. Blockchains allow efficient processing and faster transactions, saving both time and money [75,76]. Blockchain technology uses a highly secure digital signature feature to

ensure that transactions are fraud-free [77]. Blockchains enable decentralized transactions and ensure smoother, safer, and faster transactions as they are carried out with a mutual consensus of users [78,79]. Moreover, these systems enable systematic actions, events, and payments. Transactions using blockchains are immutable, i.e., they cannot be changed, edited, or altered in any way after being recorded once [80]. Hence, in addition to speed and security, blockchains also enable the establishment of trust between users and parties in a transaction [81–83].

6. Recent Exploration of MFA Applications and Blockchain Authentication

Blockchain authentication refers to the system developed for increasing the security for the users and it verifies the users and connects it to the resources found on the technologies of digital currency, digital payments, transactions, and cryptocurrencies. The blockchain mainly uses the PKC, public-key cryptography, for the encryption of wallets and also the other places or links of the blockchain where the work of value has been stored. Thus, the authentication requirements for the blockchain increase similarities between the technology itself and the measures taken for securing it [16]. Multifactor authentication is referred to as a process of verification of users through at least two authentication factors [29]. The users can make use of an additional password, flash drive, special software, some particular files, and a flash drive containing important software. The MFA works in such a way that all layers of the verification need to be cleared, i.e., the user needs to provide proof of identity through OTPs, passwords, etc. Although this method is not preferred by most internet applications due to their security risks, blockchain applications use private keys for the identification of users [84].

There are different methods and techniques for ensuring the safety of the private key. Most of the time, there is a trade-off between security and usability. One of the methods proposes the security key be placed in a device without the addition of extra security [85]. However, anyone can access the unprotected device and obtain the keys. Users may use the encryptions on these devices as they need to enable them themselves. Digital wallets are commonly used for storage and access to blockchains [86–90]. They work by encrypting the security key/s by setting up a password. However, the security and key recovery are all challenges as there are numerous attacks on the passwords and security layers applied on the wallets [85]. Another method used for increasing security is using passwords to derive a combination of keys for accessing the information on the blockchains. When following this method, the private key needs to be unlocked so that previously defined passwords can be accessed during the creation of the key. This method is also prone to some disadvantages; one of the main disadvantages is that the user will be unable to change the password. Some devices possess computing capabilities that may be used with blockchain. Although these devices do not possess or support storage and they require zero understanding of the mechanism, it is highly susceptible to malware attacks [91].

Shin et al. [92] proposed a multifactor authentication procedure for WSNs in recent network applications that act in real-time but is found to be vulnerable to the collision of users and desynchronization attacks. Ni et al. [93] presented a service for authentication mechanism for 5G enabled IoT networks using key agreement mechanism by use of an anonymous key. However, after rigorous testing, it was revealed to be a single-level authentication, despite using a complex public key cryptosystem and a single authentication method is not suitable for 5G multiservice systems [94]. A robust MFA protocol was proposed by Huang et al. [95] for systems that use fragile communications based on two standalone schemes for authentication; however, these systems are not comprehensible, making them vulnerable to access attacks. Luo et al. [96] presented a flexible 3-factor authentication mechanism for various applications based on 5G multiservice systems. In this system, four different kinds of schemes can be provided for a user to ensure identity authentication and safety. The technique was slightly costly in terms of time efficiency. These issues are addressed by Luo et al. [97], who presented a Service-Based Architecture for 5G multiservice systems that build upon the work of Luo et al. [96] and uses an adaptable

and decomposable 3-factor authentication system that can be applied simultaneously to ensure efficiency and speed. The tests on this system showed that it could provide an ideal efficiency in terms of transparency of action, security, and speed. However, further testing and real-time application are required. Wong et al. [98] also presented a 3-factor authentication scheme to ensure a high-security environment for communicating parties and integrates biometrics, password, and smart card authentication into a single system. Multiple server technologies are used to ensure that performance is quick and transparent. However, the technique still poses a communication cost.

There is limited research on the integration of multifactor analysis in blockchain-based applications. However, some papers were reviewed that can be valuable to indicate the benefits of these integrations. Antonio et al. [32] presented a multifactor analysis named 2FA for WordPress pages by using Hydro Raindrop multifactor authentication technology. In this paper, the researcher summarized the use of a blockchain-based two-factor authentication solution by a page on WordPress that contributes to securing user information. The study is not experimental, however, and the entire proposal is based on other theoretical and practical evidence. Overall, it suggested that the use of a decentralized technique provided by the integration of blockchain can enable multifactor and transparent user authentication, strengthening the security of information and the assets of individuals. Several studies also indicate the use of blockchain-based authentication procedures for autonomous vehicles [99–101]. In the study by Feng et al. [10], Blockchain-assisted privacy-preserving authentication system (BPAS) is presented to secure the data generated by vehicular ad hoc networks. This technique was proposed for ensuring accuracy as well as trust in the systems. However, there was a lack of support for batch verification in this paper that could provide an optimized verification in the form of blocks of data and hence reduce load on the resource consumption. Kebande et al. [15] also proposed an MFA based on Blockchain technology that proposed the use of an embedded Digital Signature (MFBC_eDS) that was found to be a suitable technique for countering the adversarial attacks on the Internet of vehicles in the past. Alharbi et al. [8] proposed a framework for authentication based on Blockchain technology as they claimed it could add more security to the authentication process. In this framework, the one-time password (OTP) is encrypted and sent to the application/website to complete the authentication process. This system was claimed to be safer than SMS-based authentication mechanisms, but it was less efficient in terms of time efficiency. Wu et al. [11] proposed an out-of-band 2factor authentication mechanism for IoT devices by use of blockchain to enable flexible, secure, and reliable authentication [102–106]. The overheads of blockchain use, however, were high. Table 4 summarizes all the studies related to MFA and Blockchain.

Table 4. Summary of Reviewed MFA and Blockchain Technology Papers.

Study	Technologies Mentioned			Advantage/Contribution	Disadvantage/Gap
	MFA	BC	3/4/5G		
[95]	✓		✓	A robust and effective system for fragile communications between two nodes.	Vulnerable to access attacks.
[93]			✓	The authentication mechanism for 5G enabled IoT networks in the form of a service.	Not an MFA-based technique.
[96]	✓		✓	The flexible 3-factor authentication mechanism for various kinds of applications that are based on 5G multiservice systems.	Costly in terms of time efficiency.
[92]	✓		✓	Provides a multifactor authentication procedure for WSNs in recent network applications and may be extendible to future network advancements such as 6G.	Vulnerable to the collision of users and desynchronization attacks.

Table 4. *Cont.*

Study	Technologies Mentioned			Advantage/Contribution	Disadvantage/Gap
	MFA	BC	3/4/5G		
[98]	✓		✓	Multiple server technologies are used to ensure that performance is quick and transparent.	Technique still poses a communication cost as it integrates biometrics, password, and smart card authentication.
[97]	✓		✓	An adaptable and decomposable 3-factor authentication system that can be applied simultaneously to ensure efficiency and speed.	Further testing and real-time application are required.
[32]	✓	✓	✓	Hydro Raindrop multifactor authentication technology to conduct 2FA for WordPress.	Not experimental in nature.
[10]	✓	✓	✓	BPAS for ensuring accuracy as well as trust in the systems.	A lack of support for batch verification for an optimized verification in form of blocks of data and hence reduce the load on the resource consumption.
[15]	✓	✓	✓	Embedded Digital Signature-based MFA suitable technique for countering the adversarial attacks.	Overheads are high.
[8]	✓	✓	✓	More security to the authentication process as compared to SMS-based authentication protocols.	This system was claimed to be safer than SMS-based authentication mechanisms, but it was less efficient in terms of time efficiency.
[11]	✓	✓	✓	Flexible, secure, and reliable authentication.	The overheads of blockchain use, however, were high.

7. Observations

7.1. Recent Trends and Observations

Based on the reviewed articles in this study, we observe that the MFA scheme provides an immersed level of improvement to secure sensitive data by preventing the systems from security threats. Figure 6 depicts the researchers' percentage of usage of different MFA enable mechanisms based on research studies. Almost 30% of the MFA methods were hardware tokens to highlight their importance. The soft token and OTP based on the SMS were the next important MFA enable mechanism, with almost 23% of studies employing it. While the hardware-based OTP and the authenticator applications were the less popular mechanism as adopted by almost 12% of studies only.

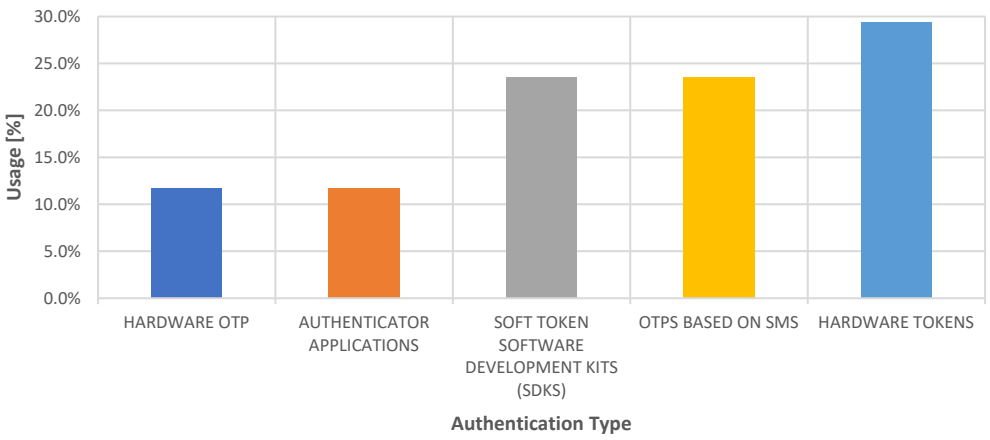

Figure 6. Trends in different authentication types to enable MFA.

Figure 7 highlights the usage of different security mechanisms for the 3G, 4G, or 5G communication technologies based on the reviewed articles. It is also observed that 67% of the reviewed papers focused on the MFA-based schemes only to provide security to different networks considering the 3G, 4G, or 5G communication networks. Additionally, only 33% of studies focused on integrating BC along with the MFA authentication schemes for securing communication networks. We observed that mostly BC-based MFA studies were conducted from 2019 onward, which is one of the main reasons for its lower popularity compared to MFA schemes. This observation also highlights that BC-based MFA schemes are less explored, and there is more room for research in this emerging field.

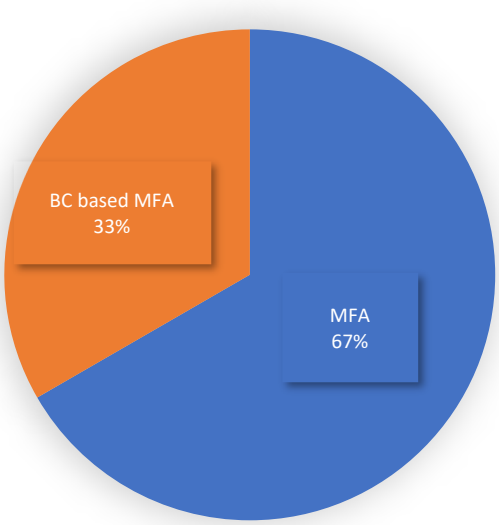

Figure 7. Adaptation of different security mechanisms for 3G/4G or 5G networks.

It can be observed that most of the studies conducted to date about the BC integration with the MFA are focused on the 5G networks. Since 5G networks are only deployed in very few countries globally, there is still a lack of research into how blockchain integration improves the MFA schemes. Security remains the prime issue in this digital world due to advancements in communication and network technologies such as 5G and internet of things networks. So, BC is a robust technology that can be integrated with the MFA schemes to provide much-needed security for future networks.

7.2. Future Research Trends and Challenges

This subsection highlights the future research trends and challenges based on the review conducted in this study. It can be observed that there is a lack of research into the application of how blockchain integration can lead to multifactor authentication in the 6G network era. However, multifactor authentication technologies implemented for 5G and prior networks can be enhanced in the 6G network in the future.

Therefore, one of the major future research trends is to examine strategies to reduce the time efficiency issues in multifactor authentication techniques proposed in the past and to increase overall effectiveness and trust in the networks. Additionally, BC-based schemes are more complex and require immense computational power and resources, which highlights one of the future research challenges for the researchers to improve the BC's computation and complexity issues to make it possible to integrate with the MFA-based security authentication schemes.

One major challenge that may be faced in this domain is that the 6G network technology is still very hypothetical and theoretical. It will be years before its implementation is materialized. Hence, researchers will need to test the proposed MFA techniques on current networks and simulation-based environments.

8. Conclusions

Conduction of a secure and reliable authentication of a large-scale transaction in the context of Internet-of-things devices is not trivial, and current network frameworks and existing security mechanisms often fall short. The MFA technology was introduced for integration in the blockchains recently. It may present a viable set of protocols and possible applications that can lead to secure transactions and efficient authentication in the 6G era. The present study reviewed the research carried out between 2015–2021 for defining and exploring the processes and strategies of blockchain, multifactor authentication, 6G, and the overall benefits through the integration of blockchain in 6G and MFA in the blockchain. The results indicate room for improvement in the 5G technologies based on the review. Additionally, the results suggest that the MFA techniques need to be integrated within the blockchain to develop new protocols and test the effectiveness of the authentication processes so that by the time the 6G technologies are developed, there are adequate authentication techniques for security. This is an essential provision as the intricacy and connectedness of the data nodes will be high in 6G technologies as they will be based on IoT.

The present review was subject to some limitations as well. First, the review was fairly generic and was performed to compile the present research on the emerging topics and technologies of MFA, blockchain, and 6G. Moreover, the current research in this domain is limited; thus, there was not a significant body of research to go through. For future researchers, it is recommended that a meta-analysis be carried out on the same topic and the applications of the MFA techniques within the 5G technologies to configure the most secure and performing strategies. The historical information can be used to test the response in the 6G technologies.

Author Contributions: Conceptualization, J.A. (Jamil Asim), Z.A., A.S.K. and J.A. (Johari Abdullah); methodology, J.A. (Jamil Asim), Z.A., R.M.S. and A.S.K.; analysis, J.A. (Jamil Asim), S.A. and S.H.; resources, S.A., S.H. and R.M.S.; data curation, M.A., J.A. (Johari Abdullah) and M.S.A.; writing—original draft preparation, J.A. (Jamil Asim); writing—review and editing, J.A. (Jamil Asim), Z.A. and S.H.; visualization, J.A. (Jamil Asim), Z.A. and R.M.S.; supervision, A.S.K., J.A. (Johari Abdullah) and Z.A.; project administration, A.S.K. and J.A. (Johari Abdullah); funding acquisition, Z.A., M.A. and M.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research at King Khalid University (KKU), under research project grant number (RGP.1/213/42).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the Universiti Malaysia Sarawak, Sarawak, Malaysia, for encouraging this research work. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University (KKU) for funding this research project Number (RGP.1/213/42).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Liu, L.; Xu, B. Research on information security technology based on blockchain. In Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis, Chengdu, China, 20–22 April 2018; pp. 380–384. [CrossRef]
2. Ehrenberg, A.J.; King, J.L. Blockchain in Context. *Inf. Syst. Front.* **2020**, *22*, 29–35. [CrossRef]
3. Abayomi-Zannu, T.P.; Odun-Ayo, I.A.; Barka, T.F. A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication. *J. Phys. Conf. Ser.* **2019**, *1378*, 32104. [CrossRef]
4. Zhu, Q.; Loke, S.W.; Trujillo-Rasua, R.; Jiang, F.; Xiang, Y. Applications of Distributed Ledger Technologies to the Internet of Things. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]

5. Zheng, X.; Sun, S.; Mukkamala, R.R.; Vatrapu, R.; Ordieres-Meré, J. Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. *J. Med. Internet Res.* **2019**, *21*, e13583. [CrossRef]
6. Hathaliya, J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the IEEE 9th International Conference on Advanced Computing, IACC 2019, Tiruchirappalli, India, 13–14 December 2019; pp. 87–91. [CrossRef]
7. Almuhaideb, A.M.; Alqudaihi, K.S. A Lightweight Three-Factor Authentication Scheme for WHSN Architecture. *Sensors* **2020**, *20*, 6860. [CrossRef]
8. Alharbi, E.T.; Alghazzawi, D. Two Factor Authentication Framework Using OTP-SMS Based on Blockchain ScaleUp View project Workflow Execution Time Predictions in Distributed Systems View project. *Trans. Mach. Learn. Artif. Intell.* **2019**, *7*, 17–27. [CrossRef]
9. Khan, A.H.; Hassan, N.U.; Yuen, C.; Zhao, J.; Niyato, D.; Zhang, Y.; Poor, H.V. Blockchain and 6G: The Future of Secure and Ubiquitous Communication. *IEEE Wirel. Commun.* **2021**, 1–8. [CrossRef]
10. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4146–4155. [CrossRef]
11. Wu, L.; Du, X.; Wang, W.; Lin, B. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. In Proceedings of the International Conference on Computing, Networking and Communications, Maui, HI, USA, 5–8 March 2018; pp. 769–773. [CrossRef]
12. Maksymyuk, T.; Volosin, M.; Gazda, J.; Liyanage, M. Blockchain-based Decentralized Service Provisioning in Local 6G Mobile Networks. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, 15–17 November 2021; pp. 516–519. [CrossRef]
13. Velliangiri, S.; Manoharn, R.; Ramachandran, S.; Rajasekar, V.R. Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications. *IEEE Trans. Ind. Inform.* **2021**. [CrossRef]
14. Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G Wireless Systems: A Vision, Architectural Elements, and Future Directions. *IEEE Access* **2020**, *8*, 147029–147044. [CrossRef]
15. Kebande, V.R.; Awaysheh, F.M.; Ikuesan, R.A.; Alawadi, S.A.; Alshehri, M.D. A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. *Sensors* **2021**, *21*, 6018. [CrossRef] [PubMed]
16. Şahan, S.; Ekici, A.F.; Bahtiyar, Ş. A Multi-Factor Authentication Framework for Secure Access to Blockchain. In Proceedings of the 2019 5th International Conference on Computer and Technology Applications, Istanbul, Turkey, 16–17 April 2019. [CrossRef]
17. Siddiqi, M.A.; Yu, H.; Joung, J. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices. *Electronics* **2019**, *8*, 981. [CrossRef]
18. Gupta, R.; Reebadiya, D.; Tanwar, S. 6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission. *Comput. Stand. Interfaces* **2021**, *77*, 103521. [CrossRef]
19. Taher, B.H.; Liu, H.; Abedi, F.; Lu, H.; Yassin, A.A.; Mohammed, A.J. A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications. *J. Sens.* **2021**, *2021*, 8871204. [CrossRef]
20. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.* **2020**, *6*, 281–291. [CrossRef]
21. Yu, J.; Wang, G.; Mu, Y.; Gao, W. An Efficient Generic Framework for Three-Factor Authentication with Provably Secure Instantiation. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 2302–2313. [CrossRef]
22. Yrjola, S. How Could Blockchain Transform 6G towards Open Ecosystemic Business Models? In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
23. Chen, X.; Ng, D.W.K.; Yu, W.; Larsson, E.G.; Al-Dhahir, N.; Schober, R. Massive Access for 5G and Beyond. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 615–637. [CrossRef]
24. Prakasam, P.; Sayeed, S.; Ajayan, J. Guest editorials: P2P computing for 5G, beyond 5G (B5G) networks and internet-of-everything (IoE). *Peer-to-Peer Netw. Appl.* **2020**, *14*, 240–242. [CrossRef]
25. Routray, S.K.; Mohanty, S. "Why 6G?". *arXiv* **2019**, arXiv:1903.04837v1.
26. Dang, S.; Amin, O.; Shihada, B.; Alouini, M.-S. *From a Human-Centric Perspective: What Might 6G Be?* Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2020; Preprint November 2019. [CrossRef]
27. Milovanovic, D.; Bojkovic, Z. 5G Mobile Networks: What is Next? *Int. J. Commun.* **2019**, *4*, 1–5. Available online: https://futurecomresearch.eu (accessed on 25 December 2021).
28. Li, Y.; Yu, Y.; Susilo, W.; Hong, Z.; Guizani, M. Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. *IEEE Wirel. Commun.* **2021**, *28*, 63–69. [CrossRef]
29. Dasgupta, D.; Roy, A.; Nag, A. Multi-Factor Authentication. *Adv. User Authentication* **2017**, 185–233. [CrossRef]
30. Dostalek, L. Multi-Factor Authentication Modeling. In Proceedings of the 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 5–7 June 2019; pp. 443–446. [CrossRef]
31. Shah, Y.; Choyi, V.; Subramanian, L. Multi-factor Authentication as a Service. In Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015, San Francisco, CA, USA, 30 March–3 April 2015; pp. 144–150. [CrossRef]
32. Cardoso, J.A.A.; Ishizu, F.T.; De Lima, J.T.; Pinto, J.D.S. Blockchain Based MFA Solution: The use of hydro raindrop MFA for information security on WordPress websites. *Braz. J. Oper. Prod. Manag.* **2019**, *16*, 281–293. [CrossRef]

33. Gupta, R.; Kumari, A.; Tanwar, S. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4009. [CrossRef]
34. Yue, K.; Zhang, Y.; Chen, Y.; Li, Y.; Zhao, L.; Rong, C.; Chen, L. A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2191–2217. [CrossRef]
35. Regulation, I. Commission Implementing Regulation (EU) 2015/2082 and 2015/2083 of 18 November 2015 Concerning the Non-Approval of Arctium. Regulation (EU). 2015. Available online: https://www.legislation.gov.uk/eur/2015/2082/adopted (accessed on 25 December 2021).
36. Das, S.; Wang, B.; Tingle, Z.; Camp, L.J. Evaluating User Perception of Multi-Factor Authentication: A Systematic Review. *arXiv* **2019**, arXiv:1908.05901v1.
37. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. Preventing DoS attacks in IoT using AES. *J. Telecommun. Electron. Comput. Eng.* **2017**, *9*, 55–60.
38. Henricks, A.; Kettani, H. On Data Protection Using Multi-Factor Authentication. In Proceedings of the 2019 International Conference on Information System and System Management, Rabat, Morocco, 14–16 October 2019; PervasiveHealth: Pervasive Computing Technologies for Healthcare. pp. 1–4. [CrossRef]
39. Copeland, M.; Jacobs, M. Reduce Cyber Security Vulnerabilities: Identity Layer. In *Cyber Security on Azure*; Apress: Berkeley, CA, USA, 2020; pp. 3–35. [CrossRef]
40. Hess, E.M.; Tolbert, M.M.; Nascimento, M.C. Vulnerabilities of Multi-Factor Authentication in Modern Computer Networks. May 2021. Available online: https://digital.wpi.edu/concern/student_works/5d86p313s?locale=en (accessed on 25 December 2021).
41. Alnahari, W.; Quasim, M.T. Authentication of IoT Device and IoT Server Using Security Key. In Proceedings of the 2021 International Congress of Advanced Technology and Engineering (ICOTEN), Taiz, Yemen, 4–5 July 2021; Research Square; pp. 1–9. [CrossRef]
42. Khan, A.S.; Javed, Y.; Saqib, R.M.; Ahmad, Z.; Abdullah, J.; Zen, K.; Abbasi, I.A.; Khan, N.A. Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. *IEEE Access* **2022**, *10*, 31273–31288. [CrossRef]
43. Dlamini, M.T.; Venter, H.S.; Eloff, J.; Blackledge, J.M.; Chetty, K. Securing Cloud Computing' s Blind-Spots Using Strong and Risk-Based MFA. Association for Information Systems AIS Electronic Library (AISeL). 2016. Available online: http://aisel.aisnet.org/confirm2016/22 (accessed on 25 December 2021).
44. Das, S.; Kim, A.; Camp, L.J. Short Paper: Organizational Security: Implementing a Risk-Reduction-Based Incentivization Model for MFA Adoption. In Proceedings of the International Conference on Financial Cryptography and Data Security, Virtual, 1–5 March 2021; pp. 406–413. [CrossRef]
45. Abiew, N.A.K.; Jnr, M.D.; Banning, S.O. Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems. *Asian J. Res. Comput. Sci.* **2020**, *5*, 7–20. [CrossRef]
46. Khan, A.S.; Abdullah, J.; Zen, K.; Tarmizi, S. Secure and Scalable Group Rekeying for Mobile Multihop Relay Network. *Adv. Sci. Lett.* **2017**, *23*, 5242–5245. [CrossRef]
47. Khan, A.S. Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network. *Int. J. Commun. Netw. Inf. Secur.* **2014**, *6*, 189.
48. Khan, N.; Johari, A.; Adnan, S. A Taxonomy Study of XSS Vulnerabilities. *Asian J. Inf. Technol.* **2017**, *16*, 169–177.
49. Sanyal, S.; Tiwari, A.; Sanyal, S. A Multifactor Secure Authentication System for Wireless Payment. *Adv. Inf. Knowl. Process.* **2010**, *53*, 341–369. [CrossRef]
50. Sinigaglia, F.; Carbone, R.; Costa, G.; Zannone, N. A survey on multi-factor authentication for online banking in the wild. *Comput. Secur.* **2020**, *95*, 101745. [CrossRef]
51. Kennedy, E.; Millard, C. Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Comput. Law Secur. Rev.* **2016**, *32*, 91–110. [CrossRef]
52. Bruun, A.; Jensen, K.; Kristensen, D. *Usability of Single- and Multi-Factor Authentication Methods on Tabletops: A Comparative Study*; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2014; pp. 299–306. [CrossRef]
53. Maciej, B.; Imed, E.F.; Kurkowski, M. Multifactor Authentication Protocol in a Mobile Environment. *IEEE Access* **2019**, *7*, 157185–157199. [CrossRef]
54. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. *IEEE Netw.* **2019**, *33*, 82–88. [CrossRef]
55. Kinai, A.; Otieno, F.; Bore, N.; Weldemariam, K. Multi-factor authentication for users of non-internet based applications of blockchain-based platforms. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 525–531. [CrossRef]
56. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
57. Khan, A.S.; Javed, Y.; Abdullah, J.; Zen, K. Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–18. [CrossRef]
58. Hewa, T.; Gur, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions. In Proceedings of the 2020 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, (6G SUMMIT), Levi, Finland, 17–20 March 2020. [CrossRef]

59. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.-T.; Pirttikangas, S. Privacy-Aware Blockchain Innovation for 6G: Challenges and Opportunities. In Proceedings of the 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, 6G SUMMIT 2020, Levi, Finland, 17–20 March 2020. [CrossRef]
60. Gürkaynak, G.; Yılmaz, I.; Yeşilaltay, B.; Bengi, B. Intellectual property law and practice in the blockchain realm. *Comput. Law Secur. Rev.* **2018**, *34*, 847–862. [CrossRef]
61. Teufel, B.; Sentic, A.; Barmet, M. Blockchain energy: Blockchain in future energy systems. *J. Electron. Sci. Technol.* **2019**, *17*, 100011. [CrossRef]
62. Khan, N.; Abdullah, J.; Khan, A.S. Towards vulnerability prevention model for web browser using interceptor approach. In Proceedings of the 2015 9th International Conference on IT in Asia (CITA), Sarawak, Malaysia, 4–5 August 2015. [CrossRef]
63. Peters, G.W.; Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond Banks and Money*; New Economic Windows; Springer: Cham, Switzerland, 2016; pp. 239–278. [CrossRef]
64. Erdem, A.; Yildirim, S.; Angin, P. Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art. In *Security, Privacy and Trust in the IoT Environment*; Springer: Cham, Switzerland, 2019; pp. 97–122. [CrossRef]
65. Khan, N.; Abdullah, J.; Khan, A.S. Defending Malicious Script Attacks Using Machine Learning Classifiers. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 5360472. [CrossRef]
66. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaria, V. To Blockchain or Not to Blockchain: That Is the Question. *IT Prof.* **2018**, *20*, 62–74. [CrossRef]
67. Andolfatto, D. Blockchain: What it is, what it does, and why you probably don't need one. *Fed. Reserv. Bank St. Louis Rev.* **2018**, *100*, 87–95. [CrossRef]
68. Khan, N.; Abdullah, J.; Khan, A.S. A Dynamic Method of Detecting Malicious Scripts Using Classifiers. *Adv. Sci. Lett.* **2017**, *23*, 5352–5355. [CrossRef]
69. Vishwa, A.; Hussain, F.K. A Blockchain based approach for multimedia privacy protection and provenance. In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; pp. 1941–1945. [CrossRef]
70. Meunier, S. Blockchain 101: What is blockchain and how does this revolutionary technology work? In *Transforming Climate Finance and Green Investment with Blockchains*; Academic Press: Cambridge, MA, USA, 2018; pp. 23–34. [CrossRef]
71. Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*; Xavier, F., Zhegu, O.M., Eds.; Edward Elgar Publishing: London, UK, 2015; pp. 225–253. [CrossRef]
72. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2018**, *57*, 2117–2135. [CrossRef]
73. Xiaolong, H.; Huiqi, Z.; Lunchao, Z.; Nazir, S.; Jun, D.; Khan, A.S. Soft Computing and Decision Support System for Software Process Improvement: A Systematic Literature Review. *Sci. Program.* **2021**, *2021*, 7295627. [CrossRef]
74. Kersten, W.; Blecker, T.; Ringle, C.M. Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. *Proc. Hambg. Int. Conf. Logist.* **2017**, *23*, 533. [CrossRef]
75. Zubair, S.; Fisal, N.; Abazeed, M.B.; Salihu, B.A.; Khan, A.S. Lightweight distributed geographical: A lightweight distributed protocol for virtual clustering in geographical forwarding cognitive radio sensor networks. *Int. J. Commun. Syst.* **2015**, *28*, 1–18. [CrossRef]
76. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Comput.* **2019**, *22*, 14743–14757. [CrossRef]
77. Faroukhi, A.Z.; El Alaoui, I.; Gahi, Y.; Amine, A. An Adaptable Big Data Value Chain Framework for End-to-End Big Data Monetization. *Big Data Cogn. Comput.* **2020**, *4*, 34. [CrossRef]
78. Lin, W.; Yin, X.; Wang, S.; Khosravi, M.R. A Blockchain-enabled decentralized settlement model for IoT data exchange services. *Wirel. Networks* **2020**, 1–15. [CrossRef]
79. Xu, R.; Nikouei, S.Y.; Nagothu, D.; Fitwi, A.; Chen, Y. BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System. *Smart Cities* **2020**, *3*, 928–951. [CrossRef]
80. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
81. Khan, A.S.; Lenando, H.; Abdullah, J.; Bin Jambli, M.N. Lightweight Message Authentication Protocol for Mobile Multihop Relay Networks. *Int. Rev. Comput. Softw. (IRECOS)* **2014**, *9*, 1720. [CrossRef]
82. Hofmann, F.; Wurster, S.; Ron, E.; Bohmecke-Schwafert, M. The immutability concept of blockchains and benefits of early standardization. In Proceedings of the 2017 ITU Kaleidoscope Academic Conference: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017. [CrossRef]
83. Kim, S. Blockchain for a Trust Network Among Intelligent Vehicles. *Adv. Comput.* **2018**, *111*, 43–68. [CrossRef]
84. Khan, A.S.; Javed, Y.; Abdullah, J.; Nazim, J.M.; Khan, N. Security issues in 5G device to device communication. *IJCSNS* **2017**, *17*, 366.
85. Eskandari, S.; Barrera, D.; Stobert, E.; Clark, J. A First Look at the Usability of Bitcoin Key Management. *arXiv* **2018**, arXiv:1802.04351. [CrossRef]

86. Dildar, M.S.; Khan, N.; Bin Abdullah, J.; Khan, A.S. Effective way to defend the hypervisor attacks in cloud computing. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017, Abha, Saudi Arabia, 26–27 March 2017; pp. 154–159. [CrossRef]
87. Chan, K.Y.; Abdullah, J.; Shahid, A. A Framework for Traceable and Transparent Supply Chain Management for Agri-food Sector in Malaysia using Blockchain Technology. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [CrossRef]
88. Balan, K.; Khan, A.S.; Julaihi, A.A.; Tarmizi, S.; Pillay, K.S.; Abdulrazak, L.F.; Sallehudin, H. RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 298–304. [CrossRef]
89. Aqeel, S.; Khan, A.S.; Ahmad, Z.; Abdullah, J. A comprehensive study on DNA based Security scheme Using Deep Learning in Healthcare. *EDP Audit. Control. Secur. Newsl.* **2021**, 1–17. [CrossRef]
90. Ahmad, Z.; Khan, A.S.; Shiang, C.W.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4150. [CrossRef]
91. Espitia, A.; Ortega, K.; Romero, E.; Jaramillo, I. Authentication and digital signature USB device for telemedicine applications. In Proceedings of the 7th International Caribbean Conference on Devices, Circuits and Systems, ICCDCS, Cancun, Mexico, 28–30 April 2008. [CrossRef]
92. Shin, S.; Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. [CrossRef]
93. Ni, J.; Lin, X.; Shen, X.S. Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 644–657. [CrossRef]
94. Ahmad, Z.; Khan, A.S.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.; Tarmizi, S.; Rodrigues, J. Anomaly Detection Using Deep Neural Network for IoT Architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
95. Huang, X.; Xiang, Y.; Bertino, E.; Zhou, J.; Xu, L. Robust Multi-Factor Authentication for Fragile Communications. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 568–581. [CrossRef]
96. Luo, Y.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. DIAM: Diversified Identity Authentication Mechanism for 5G Multi-Service System. In Proceedings of the 2019 International Conference on Computing, Networking and Communications, ICNC 2019, Honolulu, HI, USA, 18–21 February 2019; pp. 418–424. [CrossRef]
97. Luo, Y.; Li, H.; Ma, R.; Guo, Z. A Composable Multifactor Identity Authentication and Authorization Scheme for 5G Services. *Secur. Commun. Netw.* **2021**, *2021*, 6697155. [CrossRef]
98. Wong, A.M.-K.; Hsu, C.-L.; Le, T.-V.; Hsieh, M.-C.; Lin, T.-W. Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks. *Sensors* **2020**, *20*, 2511. [CrossRef]
99. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef]
100. Khan, A.S.; Ahmad, Z.; Abdullah, J.; Ahmad, F. A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. *IEEE Access* **2021**, *9*, 87079–87093. [CrossRef]
101. Khan, A.S.; Iqbal, A.M. *Mobile Multihop Relay WIMAX Networks: A Security Perspectives*; Universiti Malaysia Sarawak: Sarawak, Malaysia, 2018.
102. Saqib, R.M.; Khan, A.S.; Javed, Y.; Ahmad, S.; Nisar, K.; Abbasi, I.A.; Haque, M.R.; Julaihi, A.A. Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security. *Intell. Autom. Soft Comput.* **2022**, *32*, 1633–1647. [CrossRef]
103. Javed, Y.; Khan, S.; Khan, A.S.; Qahar, A.; Abdullah, J. Preventing DoS Attacks in IoT Using AES Static Analysis of Web Applications View project Cloud Robotics View project Preventing DoS Attacks in IoT Using AES. *J. Telecommu-Nication Electron. Comput. Eng.* **2018**, *9*, 3–11. Available online: https://www.researchgate.net/publication/322243661 (accessed on 29 December 2021).
104. Javed, Y.; Khan, S.; Khan, A.S.; Qahar, A.; Abdullah, J. EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2017**, *9*, 99–105. Available online: https://jtec.utem.edu.my/jtec/article/view/3191 (accessed on 29 December 2021).
105. Khan, N.; Ahmad, F.; Khan, S.; Abdullah, J.; Khan, N.; Julahi, A.A.; Tarmizi, S. Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2017**, *17*, 357.
106. Khan, A.S.; Lenando, H.; Abdullah, J.; Fisal, N. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *J. Teknol.* **2015**, *73*, 75–81. [CrossRef]