ISSN 2319 - 5975

Volume 13, No.2, February 2024 – March 2024

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns011322024.pdf

https://doi.org/10.30534/ijns/2024/011322024

Operational Security, Safe Quantum,Space Communications and Data Privacy Cyber Security

Priyarani A G[1], Priyanka R[2], Priyanka VK[3], Rachana N[4], Chandra Naik[5]

Students, Department of Computer Science and Engineering1, 2, 3, 4

Associate Professor, Department of Computer Science and Engineering[5]

Alva's Institute of Engineering and Technology, Tenkamijar, Karnataka, India

[1] Alva's Institute of Engineering and Technologies, India priyaannarao412@gmail.com

[2] Alva's Institute of Engineering and Technologies, India priyacs099@gmail.com

[3] Alva's Institute of Engineering and Technologies, India vkpriyanka01@gmail.com

[4]Alva's Institute of Engineering and Technologies, India rachananayak03@gmail.com

[5]Alva's Institute of Engineering and Technologies, India chandranaik@aiet.org.in

Received Date : January 15, 2024 Accepted Date : February 22, 2024 Published Date : March 07, 2024

ABSTRACT

In recent years the internet has become an important part of daily life for people around the world. 18 On the other hand, as the effectiveness of the internet increases, cybercrimes also increase. Over the last 15 years, cybersecurity has emerged as a way to accelerate the pace of change in cyberspace. Cybersecurity refers to the procedures a country or organization can use to protect its assets and information in cyberspace. Twenty years ago the term "cybersecurity" was little known to the public [1].

Cybersecurity affects not only people but also organizations or governments. In recent years, everything has been going well and it has used many technologies such as cybernetics, cloud computing, smartphones, and Internet of Things technology. Cyber attacks raise concerns about privacy, security, and financial security. Cybersecurity is a set of technologies, processes, and practices designed to prevent attacks, damage, and unauthorized access to networks, computers, operations, and machines. The main purpose of this article is to provide detailed information about types of cybersecurity, why cybersecurity is important, cybersecurity frameworks, cybersecurity tools, and problem points of cybersecurity [2].

Key words: Cyber security, Cyber-attack, Phishing, Cyber-crime, Cyber security, Internet of Things (IoT) security, Cyber security framework, Malware

1. INTRODUCTION

Cybersecurity ensures the protection and integrity of computing assets or data connected to an organization's network to protect assets from threats throughout the cyber-attack lifecycle. Currently, most economic, business, cultural, social, and government activities and interventions at all levels of government, including the interaction between people and organizations, if the government, government, and government institutions do not exist in cyberspace. Recently, many private companies and government institutions around the world have been facing cyber-attacks and poor communication. In today's technology world, protecting this data from cyber-attacks is a difficult problem. The purpose of the cyber-attack is to cause financial damage to the company[3].

In other cases, cyber-attacks may have a military or political purpose. Some of these damages include computer viruses, intellectual property damage, data services (DDS), and other attacks. For this purpose, organizations use various solutions to avoid being damaged by cyber-attacks. Cybersecurity monitors information in IT data updates in real time. So far, scientists around the world have proposed many ways to prevent or reduce the damage caused by cyber-attacks[3].

Some of these processes are in the operational phase, and some are in the research phase. The purpose of this study is to investigate and monitor the success of this model in the cybersecurity sector and examine current problems, weaknesses, and strengths of the program. Many new puppy attacks are discussed in detail. We discuss security standards and the history of early cybersecurity technologies. It also covers emerging trends and recent developments in cybersecurity, as well as security threats and challenges [12].

For IT and cybersecurity researchers, general audits are expected to be helpful. Keywords: cyber security, cyber-attack, phishing, cybercrime, cyber security, internet of things (IoT) security, cyber security framework, malware. The Internet is one of the most important inventions of the 21st century and has affected our lives. Today, the Internet has broken down all barriers and transformed the way we communicate, entertain, work, shop, make friends, listen to music, watch movies, order food, pay bills, and greet friends on birthdays and anniversaries. Our world is powered by digital information that supports critical services and infrastructure. Countries, organizations, and end users 45 are concerned about threats to the privacy, integrity, and

availability of digitized information. Security is a necessity in the digital world and permeates all aspects of our daily lives, whether public or private. Without security, the world will collapse. Attacks like WannaCry pass through unprepared citizens, businesses, and organizations, putting their jobs at risk. Cybersecurity plays an important role in technology.
Cybersecurity has come a long way in the last few years. 25 When we encounter fraud, the first thing that comes to our mind is online security.
Protecting ourselves online has become a big problem. The number of connected devices has grown rapidly in recent years and will exceed 50 billion by 2020. The increase in the number of connected devices increases the complexity of the network process, leading to an increase in network equipment. The equipment is not good. Data science has revolutionized business worldwide [13].

2 ADVANTAGES OF CYBER SECURITY

In the Internet age, organizations rely on their IT infrastructure to protect themselves from cyberattacks. As more and more organizations embrace digital transformation, so does the risk of cybercrime [2].
Cyber Security Be the knight in shining armor. A strong network security policy and architecture work together to protect computers and networks from attacks or unauthorized access. Businesses, individuals, and governments invest heavily in cybersecurity to protect their assets and information from hackers [3]. Maintain the integrity of the instructions
Data integrity refers to the reliability and reliability of data throughout its lifecycle. It can describe the status of data (such as valid or invalid) or the process of providing and maintaining correct and accurate data. For example, error checking and validation is a way to ensure data integrity in the process [7].

2.1 Units

Resolution issues required. This will allow the body to function normally and quickly recognize and prevent attacks. This document provides an overview of current cybersecurity research. We first introduce the research on network security, and in the third part, we introduce network security. IT security includes network security as a process. Cybersecurity protects digital information on networks, computers, and devices from being accessed, hacked, and destroyed. While IT security protects physical and digital data, cybersecurity protects digital data on networks, computers, and devices from unauthorized access, attack, and destruction [7].
In this section, we discuss how network security works. Brenner unveiled the first method of detecting indicators of crime in cyberspace. “Concerns” acknowledged that it is difficult to create indicators and measure cybercrime because of indicators and evidence issues, but it asked for three types of Significance: human damage and simple harm, including destruction. User argues that cybercrime creates a vicious circle when there are three types of interactions, but focuses on the identity of the attacker to identify cybercriminals, cybercrime victims, and police behavior to identify revenue as Laube[8].
It creates calculations that can determine the benefits and costs to the attacker and discuss whether it is a cybercrime. This article uses machine learning and data mining methods to perform digital queries using visual effects. The crime triangle is sometimes used to describe cybercrime and states that three variables are required for cybercrime to occur: victim, motive, and time. A victim is a person who is attacked with the motive of the perpetrator and who is not protected from the consequences of the crime that may cause bodily harm or property damage.) Non-violent attacks still exist, but there are more attacks today, and victims are based on the perpetrator's motivations such as money, violence, power, or revenge. An "opportunistic attack" is defined as an attack that targets a victim based on the victim's vulnerability. Camellia is the 128-bit block cipher recommended for this article [3].
Camellia is known for its power and high security level in software and hardware platforms. Camellia has been shown to be very safe against many cryptanalysis. In terms of software and hardware encryption speed, Camellia is as low as possible as real AES such as MAS, RC6, Rijndael, Snake and Two fish. The authors of this article use machine learning and forensic cybersecurity science to develop a method for detecting cyber threats that were previously undetectable by conventional methods[11].

2.2 Basic Cryptographic Concepts

Hashing, Decryption, and Encryption Principles Encryption is crucial to modern cryptography. Encryption uses strong encryption algorithms and keys to convert plaintext data into ciphertext to protect data confidentiality during transmission or storage. To convert ciphertext back to plaintext, a reverse process called decryption is required to access the original data. Data integrity and authentication can be verified using hashing, which creates a constant value of the input data and uses it as a digital fingerprint. Today's systems often use advanced cryptographic hashing techniques such as SHA-256 and SHA-3 to ensure data integrity.

3. SKILLS TO REDUCE THE RISK IN CYBER CRIME

Some organizations must make sure their employees get it. Although cybersecurity courses change from time to time, employees have the opportunity to hone their skills and reduce the risk of cyber attacks.

1. Network Security Monitoring
Network monitoring is an application that monitors for signs of malicious behavior or interference. It is often used in conjunction with other security tools such as firewalls, antivirus software, and IDPs. Network security monitoring can be done manually or using the software.

2. Access and Access Management (IAM)
Management of who has access to what information. Generally, administrative users have access to information, networks, and computer systems. This is network security by identifying users and controlling access. Many web security platforms support enterprise-wide IAM. IAM can be implemented in both software and hardware and often uses role-based control (RBAC) to restrict access to certain system components. With a solution like Okta, administrators can control who can access what, when, and for how long.
3. Software Security
Applications important to company operations are protected by application security. It includes controls like signatures and whitelists and helps you customize your security policies with features like data-sharing permissions and multi-factor authentication. Software security will become better with the use of artificial intelligence in network security.
4. Risk Management
Cyber security includes risk management, data integrity, security awareness and risk assessment. Assessing risks and managing the damage they can cause is a main part of risk management. The security of sensitive information is another issue related to information security.
5. Disaster recovery and business continuity Planning
Data Recovery enables organizations to continue their operations in the event of data loss, theft or corruption. This app provides models or Strategies to help businesses prevent data loss by regularly updating data and paying for the systems that manage the business
Applications important to company operations are protected by application security. It includes controls like signatures and whitelists and helps you customize your security policies with features like data-sharing permissions and multi-factor authentication. With the help of artificial intelligence in cyber security, the security of software will be better.
6. Physical security
Systems, intrusion detection devices, alarms, surveillance systems, and data destruction are some examples of body security measures. These help organizations secure their IT infrastructure.
7. Compliance and Investigations
Network security is useful when detecting suspicious situations. It also helps with management and compliance. 44
8.Security during software development
This software helps detect software flaws during development and ensures compliance with laws and standards. Cybersecurity tools carefully test, scan, and analyze software to identify bugs, vulnerabilities, or weaknesses that could be exploited by hackers or commercial competitors[3].
9. Security against DDoS
Web Security offers solutions against DDoS. It redirects traffic to other cloud-based servers and fixes the problem.
10. Protect critical systems
Network Security helps prevent attacks on large interconnected servers across multiple domains. It allows users to measure cybersecurity depending on their devices, by following industry standards and strict security standards. It monitors all applications in real-time and constantly evaluates network security, servers, and users[9]. Applications important to company operations are protected by application security. It includes controls like signatures and whitelists, and helps you customize your security policies with features like data sharing permissions and multi-factor authentication. With the help of artificial intelligence in cyber security, the security of software will be better. Cyber attacks and cyber warfare attacks must have a political or security purpose.

4. CYBER WARFARE EVALUATE SITUATIONS:

(1) State-sponsored cyber espionage to gather information to plan future cyber attacks,
(2) Cyber attacks aimed at laying the foundation for all attacks and popular attacks,
(3) Cyber attacks aimed at disabling attacks. devices. Physical attacks,
(4) Cyber attacks promoting physical attacks, and
(5) Cyber attacks with the ultimate goal of mass destruction or disruption (cyber warfare) .
One of the types of cyber attacks is encryption. Encryption is a reverse method of encrypting data that requires a key to decrypt. Encryption can be used in conjunction with encryption to provide another level of privacy . Encryption is the use and study of encryption and
decryption of information so that it can only be decrypted by someone[4].
A system that encrypts and decrypts data is an encryption system. Encryption is a powerful tool to protect important personal information from threats from strangers and criminals and to hide illegal activities from the police. As computers become faster and encryption systems become more secure, cryptographic algorithms need continuous integration to avoid insecurity. Note that in general a distinction can be made between cybercrime, cyberwar, and cyberattack. explain the difference between cybercrime, cyber warfare, and cyber-attack by describing the different concepts between them.
Cyber War Cyber warfare is the most advanced and sophisticated cyber-attack (cyber operation) against the national cyber interests of many countries and will have the greatest consequences[6].
Cyber defense covers all non-military connections and networks in a country to protect, protect, prevent, timely investigate, and create effective responses to cyber-attacks. uses non-communication facilities. biome refers to the development of countries supported in various local dynamic network environments.
A virus is a self-help program that replicates itself to infect other files and other programs and can cause programs to malfunction. Computer viruses act like viruses and infect cells in the host's body by dividing. Some popular viruses are NIMDA, SLAMMER, and SASSER.
Hacker A person who enters a system or gains access to information without permission to view, copy, modify, delete, or destroy the system. Damage is not taken into account in this section (Cao et al., 2019). Also, in terms of the perpetrator of

the attack, only the state is usually mentioned, but if the public protest is within the context and domain of state control and decision-making (state-controlled cyberspace), then it is not state and private. The law of filing a lawsuit against this must be different because the lawsuit of both parties against our country that does not fall under the above provisions will not be covered. Considering this situation, it can be said that the above points are often incomplete and do not include an important part of the struggle of private and non-governmental organizations that create the machine vacuum .

Differences Between Cybercrime, Cyberattack, and Cyber Warfare [6].

More and more information is digitized and accessible using the Internet and wireless and wired digital communications. One of the main reasons for this is the rapid change in technology and the increasing use of software in various fields such as finance, government, military, retail, hospitals, education, and energy. Since cybercriminals use all sensitive information, this information must be protected with cybersecurity [8].

Cybersecurity protects sensitive data and critical systems from online threats. Network security measures sometimes referred to as information technology (IT) security, are designed to protect against threats from within or outside the organization [13].

5. DATA PRIVACY

In the example of Recital 4 of the GDPR and Recital 2 of the Procedural Directive 1995/46/EC, the main purpose: "The processing of personal data should be aimed at serving humanity." For this purpose: the Data Controller warrants Compliance with the law, legal justification for data processing based on necessity (not just convenience of processing), and proportionality [7].

For example, for the collection of high-risk health data, GDPR requires him to conduct a DPIA and assess the level of risk, including whether the data should be processed, to reduce the risk [9].

Through data protection legislation, the UK and EU demonstrate cooperation, ethics, and transparency with robust controls to curb data breaches.

However, also draws attention to the diversity of legal frameworks and the movement of people around the world in general. it should provide information

5.1 Data Privacy: Consent-Contact Tracing Apps

In the Republic of Ireland survey of over 8,000 respondents, 54% said they would be open to using the contact tracing app. Similarly, in a survey of 4,444 of 2,000 participants in the UK, 55% said they would accept the use of government-run apps, with 4,444 using the NHS contact tracing app in particular.

This information shows that the remaining 45% of the UK population does not use apps, which could impact the government's ability to effectively manage data collection and processing of critical health information.

There is a gender[7].

In contrast, in other countries, public consent is a prerequisite when data collection is initiated in the public interest. This means that data access from 4,444 individuals is also supported by the government. Amnesty International (2020) also draws attention to many instances of questionable data protection practices in many countries. These examples justify a more focused and intensive approach to collaborative research on privacy, as they have the potential to demonstrate the extent of awareness and attitudes about privacy, as well as their interpretations. Learn how to effectively apply powerful s and scalable results by analyzing different legal and regulatory frameworks, solutions, and practices during pandemics and crisis situations. For example, the urgently needed effort to distribute Covid-19 vaccines to all countries requires robust and transparent data.

5.2 Data Protection

Data Protection: Legal Framework [UK-EU] Between the UK and the EU, the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR) work together to protect businesses, organizations and governments. We are monitoring how they work together.

Use of data Use of personal data. eight core objectives guide all those responsible for sharing and processing personal data: data must be lawful, fair, accurate, up-to-date, and not stored longer than necessary. We strictly state that you must not do this, keep it safe and secure, and that you cannot forward your. Outside the European Economic Area (EEA).

The GDPR is human rights-encompassing in nature and has additional data collection and processing principles (e.g. Purpose, data type, processing period)[7].

5.3 Data Privacy Laws

Privacy laws are laws that govern the collection, use, disclosure, and protection of personal information and data. 9 These laws are designed to protect individuals' personal information and ensure that it is collected, used, and used only for legitimate and lawful purposes. Re-formulation Approved purpose will be disclosed. Data protection laws may vary by country or region, but many have similar requirements and principles. For example, many data protection laws require businesses and organizations to obtain consent from individuals before collecting personal information, give individuals control over their personal information, and ensure that personal information is treated and stored securely. 10. This includes the right of individuals to access their data, to have any errors or inaccuracies in their data corrected, and to request the erasure of their data. Data protection laws also generally require businesses and organizations to be transparent about how they collect, use, and disclose personal information, and to provide individuals with clear and understandable information about their data protection rights and options[8].

6. ABBREVIATIONS AND ACRONYMS

As mentioned above, key terms such as confidentiality, integrity, and availability are often used to describe access to a system. It must be recognized that no system or environment is completely secure, regardless of security procedures, standards or technology. Cybersecurity is fun. Your company or organization faces new threats every day. For example, new technologies are constantly being developed to protect against threats. Anyone who follows the news knows how the business world manages cybersecurity[10]. Schools and organizations around the world withhold information until a ransom is paid. Cybersecurity is not just an IT problem. In fact, its scope is very broad. Everyone knows about the internet these days. Even illiterate people use smartphones and they have become an important part of daily life. T5h1ey is not exaggerating when someone says people are online today. At the same time, the internet has become an important part of people's lives. However, companies often have a central security department responsible for cybersecurity policies, standards and solutions. The company's safety department's standards and solutions become guidelines for regulations. In cases where security is the most important aspect of the organization, you can also see the cyber security policies published by various organizations in the wing of Congress. These common elements sometimes reveal conflicting policies that result from trying to address these issues simultaneously [9].

The country's cyber policy is now part of its national security policy. Even if we think that a country's cyber security policy is in line with the Ministry of Justice or economic policy, these rules and regulations are not the same as the law. In fact, the law is created through discussions and debates from different angles and published in reports and lectures. The law is designed to guide and set rules and regulations. The law itself has nothing to do with rules.

Laws, treaties, and policies represent effective and efficient authority at best. However, cybersecurity enforcement orders, policies and regulations can also be issued without establishing a cybersecurity policy.

In a business setting, different departments have to abide by the rules for fear of punishment until the offending department is shut down. For example, coding HR, demographics or pricing policy, and failure to comply with notification rules will close the relevant section.

Middle management supports processes such as recruitment or debt collection and is expected to incorporate communication policy into the workplace and establish department-level measures to measure compliance. In the public sector, the integration of all aspects faces regulatory constraints [9].

7. QUANTUM CRYPTOGRAPHY: THEORY

To understand QKD, we first need to move away from the traditional key distribution metaphor of Alice sending specific keying material to Bob. Instead, consider a more symmetric starting point in which Alice and Bob first create their own independent random binary sequences using the surplus amount of key material they eventually share. is required. Through public discussion, it is possible to perform bit-by-bit comparisons of sequences using quantum transmission (via "quantum channels") and publicly discuss the results (via authenticated public channels). agrees to QKD protocol. Common random subsequences are distilled around them and serve as a key material. It is important to realize that it is not necessary to identify all shared numbers or specific numbers, as the only important requirement is that the numbers must be secret and random. Several QKD protocols have been developed, but for simplicity, we will discuss the B92 QKD protocol [7], which is minimal in terms of preparation and measurement of the polarization state of a single photon. (Cryptographically, the BB84 protocol has certain advantages, but the physical issues associated with it are the same as B92[6].

7.1 Experimental Point-to-Point Quantum Key Generation over 0.5 KM in Daylight

The success of QKD on free-space optical paths relies on the transmission and detection of single photons against a high background through turbulent media. These are difficult problems, but they can be overcome by careful selection of experimental parameters and by using a variety of optical techniques developed for laser communication. The atmosphere has a "window" of high transmittance to light at wavelengths around 770 nm. Photons at this wavelength can be easily generated using robust, low-power semiconductor lasers, and their polarization properties can be controlled using commercially available His optical components. Additionally, commercial single photon counting modules (SPCMs) are now available that can count such photons with up to 65% efficiency at rates of 1 MHz and dark counting rates of 50 Hz[14]. The atmosphere is inherently non-birefringent at these wavelengths, allowing it to faithfully transmit QKD polarization states. However, atmospheric turbulence causes both photon arrival time jitter and beam movement (due to changes in the refractive index). Due to the slow time scale of turbulence (0.1 s to 0.01 s), jitter can be compensated for by applying brightly timed laser pulses (which do not carry important information) at different wavelengths for short periods (e.g., 100 ns))[12]. All QKD photons are transmitted. Once this bright pulse arrived at the receiver, the atmospheric propagation time did not change over the short intervening interval, allowing us to establish a well-defined time window for the arrival of a single QKD photon. Beam movement caused by atmospheric turbulence reduces the QKD bitrate, but as we will see later, even if uncontrolled it is not a significant constraint on the surface-to-satellite path. yeah. However, for laser communications, active beam steering methods ("tip-tilt" control) have been developed to direct the beam to the receiver. For example, by monitoring the reflected component of the bright temporal pulse, an error signal can be derived and fed back to the beam steering mechanism. At first glance, a more serious concern is that the large background of photons from the Sun (or the Moon at night) could obscure her QKD

signal of single photons. However, as discussed below, (sub-)nanosecond timing, narrow wavelength filters, and small solid angles for photon acceptance (spatial filters) at the receiver. You can reproduce this by combining: Background is manageable [7].

7.2 Quantum Key Distribution to Satellites

Quantum Key Distribution to Satellites The proof-of-concept QKD demonstration on a horizontal ground path provides strong evidence that surface-to-satellite QKD is possible.
Paraphrase This is because optical turbulence effects are the main hurdle to overcome in ground-based satellite QKD, and turbulence effects mainly occur in the lowest 2 km of the atmosphere. Ground-to-satellite and satellite-to-satellite QKD should be possible for both low-Earth orbit (LEO) and geostationary satellites. For illustrative purposes, we estimate here the significant QKD generation capability via an overhead pass (required approximately 8 minutes) between a ground station and an LEO satellite (approximately 300 km altitude)[10]. Our goal is to create several new cryptographic variables, each a few hundred bits long. Assume that the QKD transmitter (Alice) is at the ground station and the receiver (Bob) is at the satellite.(Similar arguments support the feasibility and hardware advantages of his QKD transmission from satellite to ground.)[13].

8. CONCLUSION

Cyberspace and other technologies are the most important energy sources of this century. In cyberspace, low cost, anonymity, vulnerability and inequality create explosive power; thus breaking the law. Criminal groups and individuals and even the government play an important role here. Of course, this phenomenon does not affect the national security of the government. 21 This effect can be measured in several ways.he first is the concept of security. National security cannot be defined by military issues and internal and external borders, but today it is the risk of lowering the quality of life of the affected population when it comes to national security. Second, the elimination of the cyber threat in the region. Military threats were unique in the past. So it is not easy to deal with, or at least to analyze[1].
Third is the level of vulnerability created by cyber threats. As these threats are different, diverse and related to cooperation and development, the level of harm is very high. Fourth, these threats cannot be contained by conventional measures such as the army and police alone, the government alone is not sufficient to deal with the threats. He asked her to face 38 threats while she was with them. Fifth, as the previous points have shown, cyber threats are not limited to governments, individuals and businesses do not protect them. Sixth, because security in the information age is more than national security, many of the government's 4,444 international affairs systems can easily be overlooked or confused. The network also ensures good production and good distribution of knowledge in the community. No matter what application or business the network is used for, scalability is always a consideration[9].

REFERENCES

1. Cybersecurity, Data Privacy and Blockchain: A Review, 12 January 2022
2. Systematic and Critical Review of RSA-Based Public Key Cryptographic Schemes: Past and Present Status. IEEE Access, vol. 9, 2021
3. Gallaher MP, Link AN, Rowe B. Cyber security: economic strategies and public policy alternatives.
4. Chain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017,2017 IEEE global communications
5. On the compatibility of adaptive controllers
6. Magnetization reversal in films with biaxial anisotropy.
7. Artificial intelligence and machine learning within the context of cyber security used in the UK SME Sector. In: AMI 2021— the 5th advances in management and innovation conference 2021.
8. Covid-19 Crisis: Is our Data Likely to be Breached? In AMI 2021 – The 5th Advances in Management and Innovation Conference 2021.
9. Parametric study of thermal and chemical nonequilibrium nozzle flow, M.S.
10. Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution
11. Active vs Passive Cyber Attacks Explained | Revision Legal, 2017.
12. An Explanation on Different Types of Attacks in Modern Cryptography System.
13. A Survey of Man in the Middle Attacks, IEEE Communications Surveys and Tutorials. 2016.
14. Blocking of Brute Force Attack.
15. GDPR compliant blockchains-a systematic literature review. IEEE Access. 2021;9:50593–606.