VOLUME 4 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

AN ANALYTICAL STUDY ON HOW BLOCKCHAIN CAN PREVENT CYBERCRIME IN REAL-WORLD SCENARIO

- Dev Dutta & Neha Gupta[1]

Abstract

The advancement of science and technology connects people throughout the world. The Internet has been introduced in the 1900s, and the invention of the computer is a recent advancement in science. The development of computer technology has accelerated humankind's progress. Information technology and computers have progressed quickly over the past 50 years and have taken control of almost every aspect of human civilization. The development of computer technology has had an impact on crime as well. A new kind of crime termed cybercrime evolved in society as a result of computers providing new ways and means to break the law. As the internet has given access to all the human of everything while sitting in the corner of the room, from doing grocery shopping to studying online, it makes life very easier, but it has a negative point also as crime has happened online, they are now advanced in the technology as well.In this paper, we get to know how can we implement blockchain technology into action to fight against Cyberattacks. A blockchain is a distributed ledger that is completely open to anyone. Blockchain technology describes a decentralized database system with digital asset blocks that are cryptographically linked together. Blockchain technology has the ability to be used in a wide variety of applications. Utilizing its integrity guarantee to provide cybersecurity remedies for several other technologies would be among its finest uses. Industries across the globe are adopting Blockchain technology for security purposes. Later in the paper, we will get to know about the real-life implementation of the technology and some complications and how to overcome them.

Cyber Crime

[1] Student at The University Of Calcutta

Cybercrime refers to any illicit activity carried out online. Cybercrime which includes everything from electronic theft to denial-of-service attacks is a broad term used to describe criminal activities in which computers or computer networks are a tool, a target, or a location. It's a catch-all phrase to crimes like sabotage of computer systems and 'networks', Theft of data/information stealing of credit & debit cards, and so on. In 2021, India Home to the 4th Highest number of Cybercrime victims in the world[2].

The first case of Cybercrime was documented in 1973. Using a computer, a bank teller in New York stole $2,000,000. The first spam email was sent in 1978[3].

Cybercriminals target individuals' personal information as well as data of the companies for sale and theft. Technology transformed Society beyond expectation after the introduction of the internet, it made human life more convenient and also helped different Sections of the world to come closer Culturally, Socially, and economically. The Internet has put an end to all the barriers of time and space.

Cybercrime is so challenging to manage and combat due to its global Scope. We now have a wealth of advantages because of the development of technology it provided us with several benefits that will help us tackle current issues and expand quickly, but it also gave the scope to criminals to commit crimes with the least chance of risk of detection. Cyberspace has benefited the aberrant behaviour in society. The idea of cybercrime has grown quickly, and we are now dealing with serious menace to global society from its effect. The State of Human Society has deteriorated due to cybercrime as society becomes more and more reliant on technology[4].

The Doctrine of Mens Rea & Actus Rea

The two most crucial components of crime in terms of Traditional crimes are 'Mens Rea &Actus Rea' such effect of human activity as the Law want to avert is what Actus means. For there to be a crime, there must be a commission on omission. Mens Rea refers to "A guilty state of mind" in Legal terminology. The Second essential component of crime is the mental

[2]Federal Bureau of Investigation, Internet Crime Report 2021,<https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf>accessed on 07/10/2022

[3] Sauvik Acharjee, The History of Cybercrime: A Comprehensive Guide(2021)<https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/> accessed on 07/10/2022

[4]Prof RK Chaubey, "An Introduction to Cyber Crime and Cyber law" (Kamal Law House 2021) accessed on 07/10/2022.

state that renders it "reus", making it unlawful. Almost all crimes require evidence of some form of mental component. It is extremely challenging to ascertain the Mens Rea in cybercrimes.

In cybercrimes, It is crucial to ascertain the hacker's mental state and regardless of whether they knew about it that the access was unauthorized.

As a result, it is sufficient that the hackers gained unauthorized access to "any computer and not just a "particular computer" where the hacker is an outsider and lacks the authorization to access it, it is simpler to demonstrate his awareness of this. To prove that a hacker exceeded his bounds and was even aware of what he was doing. So, however, is difficult when the hacker already has a restricted amount of authority, as in the case of an employee of a corporation. Actus Reusability in cybercrimes has grown difficult because the entire act is carried out in intangible settings. Although it becomes a herculean endeavour for the law, the culprit may still leave some footmarks in the machine, the necessary enforcement mechanisms' physical form, or in a manner that, at the very least,is acceptable in evidence[5].

Consequences of Cybercrimes

McAfee report, globally the impact of economic losses due to cyber-crimes is estimated at $1 trillion. Worldwide losses due to cybercrime were over $1 trillion, more than 50% has increased from the year 2018. In 2019, the same kinds of incidents were reported by two-thirds of the companies of cyber-attacks[6].

Economic harm is one of the lucid outcomes of cybercrime, and it can be quite significant, However, cybercrime also has a number of additional catastrophic effects on enterprise, including:

After a security breach reduces a company's worth, Venture Capitalist perspicacity can become a major issue.

Following a security breach, businesses may have higher borrowing costs and may have difficulty raising more revenue.

[5]Dr Talat Fatima, Cyber Crimes (Eastern Book Company 2021) accessed on 07/10/2022
[6]McAfee and CSIS Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact, *Press Release | McAfee and CSIS Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact.* (2020) <https://www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629>accessed on 08/10/2022

Penalties and fines for failing to protect clients from data include loss of sensitive consumer data. Data breaches may result in legal action against the business.

Due to casualties, cyberattacks hampered brand identity and dignity and break the credence of the users.

Businesses not only lose their current users but also find it problematic to acquire new users.

Direct costs may also be sustained such as the price of recruitment, cybersecurity firms for remediation, higher insurance premium rate, public relations (RPR), and other expenses could be incurred[7].

Safety Measures Against bloodless crime

New strategies are required to address the issue of high-tech crime due to the global nature of cybercrime. In addition to the cyber laws, the following things should be considered while utilizing the Internet to ensure our online safety:

At the gross roots level, the afterness of cyberattacks and cyber legislation should be raised among learners. Cyber literacy should be taught to learners in the computer centre, in academics and in universities as well. Any educational establishment can throng a cyber-law awareness workshop to enlighten the learners with a basic understanding of the internet and its security[8].

Who Commits Cybercrime?

One of the modern crimes with the quickest rate of growth is cybercrime. According to cyber experts, roughly around 1 million potential cyber-attacks are attempted every single day, and with the advancements of portable telephones and cloud technologies, this number is likely to expand 'To help mitigate for growing, businesses and companies, cooperations have been expanding their cyber security teams and efforts[9].

[7]Muskan, 'What Is Cybercrime? Different Types and Prevention' (Intellipaat Blog) <https://intellipaat.com/blog/what-is-cybercrime/>accessed on 08/10/2022
[8]Vedang Upadhayay, 'Cyber Crime in India' (*legalservicesindia.com*, 31 October 2021) <https://www.legalservicesindia.com/law/article/2266/6/Cyber-Crime-In-India?id=2266&u=6>accessed on 08/10/2022
[9] P Seemma, S Nandhini and M Sowmiya, 'Overview of Cyber Security' (2018) Vol. 7(Issue 11) IJJRCCE 5, accessed on 09/10/2022

It involves activities like child sex, organ or activity printing, credit card fraud, cyberstalking, online libel, unauthorized access to computer systems, disregarding copyright, software licensing, and trademark safety to protect, disabling encryption to make unlawful copies, software piracy and taking someone's else identity to commit a crime. Those who carry out such crimes are called cyber criminals.

Cybercriminals are so-called hackers of four different types, such as:

1. Pure Hackers
2. The Cracker
3. The Phreaker
4. Cyber Punk

Pure Hackers – Many of these people have explicit degrees of financial backups from which they spend their time pondering around various networks. Whatever, pure hackers do is not considered to be legal because any intrusive attempt into any network is considered as 'hacking', even if they do not lay any damage or perforate any systems, but this does not make them protected from any legal actions. In fact, it remains illicit to break into a computer network and can cause damage to the system due to its inexperience.

The Cracker – The word "cracker" applies to criminal hackers or pirates. They took advantage of their skills on grounds to get pecuniary aid, and to harm organizations or an individual. Cracker exists in different forms. It includes everything from the 'little hit' to government cyberterrorism via organized crime, the Russian mafia, and drug cartels are a few examples. These crackers are all participants in the war of information. As the value of information in the economic fight increases their numbers keep rising.

The Phreakers – It more specifically relates to those who specialize in phone hacking on ad worldwide web. Their action might or might not be regarded as criminals.

Their principal function is to root the Telephone line by cutting off some network lines. These competencies often permit them to abscond from Law enforcement. To have fun and win money. Scam phone operators engage in this activity. Since they deduct the cost of their telephone bill and keep going skimming from networks in a more subdued manner, many serious hackers are phreakers. The urgency of the internet and the significant fall in the worth of Telecom cost has been remediating a huge part of this problem. In spite of everything, there are still phreakers who take up the task of hacking the telephone web.

Cyber Punk – These peoples are masters and experts in encryption or decoding data[10].

Cybercrime Techniques

These are a number of techniques that criminals want to acquire individual personal and private networks.

Some of the most common are: -

- Botnet – A purposefully designed web of bots known as a "botnet" shows the web's back end to transmit malware undetected.
- Zombie Computer – A computer that has been purposefully compromised by cybercriminals in order to access and/or attack a private network is known as a zombie computer.
- Distributed Denial of Service (DDoS) – DDoS Strom, cybercriminals dos not necessarily look for access data, but rather they are hoping to block the network to a complete halt by flooding useless files and data. DDoS attacks such as the one that took down popular websites such as Twitter, Spotify, and Amazon on Friday, 21st October 2016 are such cases.
- Metamorphic Malware – One of the more Avant-grade techniques, is 'Metamorphic Malware', which constantly modifies its codes, making it highly difficult to detect by even the most precocious anti-virus software. According to experts, malware that can infiltrate networks steal data and conceal its actions will continue. These types of malware will hinder Law enforcement's ability to track down and prosecute offenders and make it harder for businesses and government entities to determine how much data has been tampered with[11].

What is Cyber Security?

Cybersecurity is a domain that is built to eradicate cybercrime. 'IT' security is also referred to as cybersecurity. Cybersecurity is the backbone of network and information security. Security

[10]National Agency for Information And Communication And Technology, 'Types of Cybercriminals' (*www.antic.cm*) <https://antic.cm/index.php/en/security/cybercriminality/222-cyber-criminality-types-of-cybercriminals.html>accessed on 09/10/2022

[11]Norwich University Online, 'Who Are Cyber Criminals?' (*https://online.norwich.edu/*, 13 February 2017) <https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals>accessed on 09/10/2022

which is built to maintain confidentiality, integrity, and availability of data, is a subset of cybersecurity[12].

Cybersecurity is the activity of defending systems and networks against online assaults that try to view, alter, or delete digital data in order to steal money or private information. The need to strengthen security measures to safeguard digital data and transactions grows. Malware such as viruses, Trojans, Rootkits, and other types of malware can be used to carry out cyberattacks. Phishing, Men in the Middle (MITM), Distributed Denial of Service (DDoS), SQL Injection, and Ransomware attacks are a few examples of frequent cyberattacks.

Why do we need Cyber Security?

At present, we live in a 'Digital Era' where all of our lives depend on the internet, computer and electronic medium.

In Today's scenario, all infrastructure like healthcare, financial banking system, government and manufacturing industries use technology, and all of the sectors are well connected to the internet web. Some of their information, including their intellectual property, financial information, and personal data, may be sensitive to illegal access or exposure, which could have unfavorable effects. With this knowledge, trespassers and threatening actions can penetrate them for monetary gain, extortion, political or social purpose, or just vandalizing.

Cyberattack is now a worldwide concern that hacks the systems and other security attacks could be in danger. Therefore, to safeguard data from well-publicized security breaches, it is crucial to establish a vigorous cybersecurity plan.

Moreover, the volume of cyberattack strikes organization and companies which particularly deals with data, pertaining to personal or financial records, health records, or national

security must implement robust cybersecurity procedures and measures to safeguard their sensitive businesses and personally identifiable information[13].

Counter-measures against Cyberattacks

[12] Muskan, 'What Is Cybercrime? Different Types and Prevention' (*Intellipaat Blog*) <https://intellipaat.com/blog/what-is-cybercrime/>accessed on 09/10/2022

[13] P Seemma, S Nandhini and M Sowmiya, 'Overview of Cyber Security' (2018) Vol. 7(Issue 11) IJJRCCE 5,accessed on 09/10/2022

To safeguard from cyberattacks there is a number of counter-measures that cybersecurity professionals can implement:

- Network Encryption – Network encryption is a security mechanism used at the network level to encrypt data so network access limits to the authorised data processors.
- Proxies – Proxy servers are a type of security measure that links users to a distant place where their data and information are encrypted. By manipulating the transmitted information, users of proxies can give a potential hacker the chance to obtain inaccurate or erroneous information.
- Firewall – A network wall known as a firewall aids users in preventing access from unreliable sources.
- Cyber liability Insurance – Cyber liability insurance is a form of legal defence that can shield a company or organization from responsibility in the event of a data breach. With the rise in the number of social security and credit card numbers stolen, cyber liability insurance has become crucial. One of the drawbacks of technological growth is the rise of cybercrime. Cybercriminals are rising using the highest quality tools and tactics to carry out well-coordinated attacks on the web. Information security professionals should adopt a comprehensive strategy to safeguard their infrastructure in order to help, prevent, and defend against future cybersecurity attacks, including counter-measures like network encryption (protocols infographic), proxies, firewalls and cyber liability insurance. Cybersecurity should continue to be proactive in keeping up with the most recent methods and tools available in the sector for defending against cyberattacks[14].

What will be the benefits of Cybersecurity?

Cybercrime has reached far and wide, with the rapid growth of technology. Cybercrime worldwide costs the global economy $375 billion per annum.

Here are the benefits of implementing:

- Cyberattacks and data breaches for industries.
- Data and network are protected.
- Illegal access to the user is avoided.

[14]Norwich University Online, 'Who Are Cyber Criminals?' (*https://online.norwich.edu/*, 13 February 2017) <https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals>accessed on 09/10/2022

- Fastest recovery time after a breach.
- Improved company credentials with the correct security controls in place.
- Improved shareholder confidence in information security arrangements[15].

2022 Must Know about the Cyberattack

Attacks on the server, have been rated the 5th top-rated threat in the year 2020 and become the new norm across the private as well as public sectors. For various Industries, it is a big menace growing in 2022 as these IoT cyber-attacks are expected to be doubled by the year 2025. Plus, the year 2020 report by the World Economic Forum states the rate of detection is as low as 0.05% in the United States.

Cybercrimes, which consist of everything from stealing or embezzlement to hacking data and destruction, during Covid-19 cyberattacks is up to about 600%, nearly every sector has had to embrace new tactics and it forced companies to adapt to the internet whether it's a small business or growing start-up[16].

Costs of Cybercrime

By 2025, according to predictions, cybercrime will cost businesses worldwide around $10.5 trillion yearly, up from $3 trillion in 2025. According to cybersecurity ventures, cybercrime constitutes the largest ever transfer of economic wealth, growing at a price of 15% year over year.

In 2014, $300 billion was approximately damaged caused by cybercrimes.

In 2015, $400 billion in cyberattacks cost industries every year[17].

Impact and Severity of Cyberattacks

An enterprise may experience a range of effects from modest operational delay to significant financial losses as a result of cyberattacks. Every result of a cyberattack, regardless of its sort, comes at a cost, whether it be monetary or otherwise.

[15]JavaTpoint.com 'What is Cyber Security? Definition, Types and Importance - javatpoint' (*www.javatpoint.com*) <https://www.javatpoint.com/what-is-cyber-security>accessed on 10/10/2022
[16]Mike Mclean, '2023 Must-Know Cyber Attack Statistics and Trends.' *Embroker.com*<https://www.embroker.com/blog/cyber-attack-statistics/>accessed on 10/10/2022
[17]Bsigroup.com, 'Cyber Security - Protecting Networks, Computers and Data' (*https://www.bsigroup.com/en-GB/*) <https://www.bsigroup.com/en-GB/Cyber-Security/>accessedon 10/10/2022

After several weeks or even months have passed, the effects of the cybersecurity incident may still have an influence on your business.

Your business may suffer in the following areas:

- Losses in funds.
- Reduction in productivity.
- Tarnished reputation.
- Legally responsible.
- Difficulties with business continuity.

Attacks by ransomware becoming a bigger problem[18].

In the year 2016, businesses fell victim to every 40 seconds of attack of ransomware. According to a survey by Cybersecurity venturer, this is anticipated to increase to every 11 seconds by 2022. When malicious software is used to block access to a computer system or data, the victim is held hostage until the criminal demand a ransom.

Cybercrime is ubiquitous and ineluctable! – Bugs are omnipresent, what should you do to avoid falling prey to malware, ransomware, and online crime?

As it is well known, cyber scams are on the rise and spreading like a rage of fire all over the world, especially given the current distant working environment brought on by the global epidemic. At this time period, it's crucial to establish the industrial hawk and secure data from cybercriminals.

Let's start by being shrewder than the criminals.

However, let's first have a look at a few facts:

- 1 out of every 5 industries that paid the ransomware never received their files back.
- Every 39 seconds, ransomware targets big companies and hacked their data and server[19].

After taking all the measures and preventive steps are we all safe from the cyberattack?

[18]Mike Mclean, '2023 Must-Know Cyber Attack Statistics and Trends.' *Embroker.com*<https://www.embroker.com/blog/cyber-attack-statistics/> accessed on 10/10/2022

[19]Cyber laws and Information Security Advisors., '11-ways-to-protect-yourself-against-cybercrime' (*https://www.cyberralegalservices.com/*) <https://www.cyberralegalservices.com/blog/11-ways-to-protect-yourself-against-cybercrime/>accessedon 10/10/2022

Well, Cybercriminals are the masters of computer technology even after all the countermeasures, are big industries and IT sectors safe?

Well, In October 2016, one of the largest domain (DNS) providers, experienced a major (DDoS) denial of service attack that interfered with many high-profile websites with high traffic such as 'Netflix', 'Twitter', and 'Spotify'. Cyber risk specialists from 'Deloitte', suggest that the organization adhere to secure, observant and resilient behaviour when handling cybersecurity regardless of the advanced technology[20].

With the increasing number of cyberattacks, hackers are becoming more advanced and sophisticated. Applying Decentralized technology 'blockchain' would prevent vulnerable single points exploited by hackers or pirates.

Blockchain Technology

As the head stated that a blockchain is a chain of information containing blocks. This technique was initially developed in the year 1991 by a group of researchers with the intention of timestamping digital documents to prevent forgery or backdating, pretty much like a notary[21].

However, it remained mostly unused until the year 2009, then it was adopted by "Satoshi Nakamoto" to lunch the virtual currency 'Bitcoin'[22].

A blockchain distributed ledger that is totally accessible to everyone is called Blockchain. When data is entered into a blockchain, they have an intriguing quality that becomes exceedingly impossible to change it.

Blockchain technology is specifically made to be profitable over time. Blockchains are highly encrypted, irreversible data blocks that provide the ability to combat any fraud.

With the aid of top-notch security standards, blockchain technology also protects encryption keys.

[20]Eric Piscini, David Dalton and Lory Kehoe, 'Blockchain & Cyber Security' Deloitte EMEA Grid Blockchain Lab 14, accessed on 10/10/2022

[21]Mohammed Qasim Obayes, 'Blockchain and Cyber Security' [2021] Emam Reza University of Mashhad Faculty of Engineering Computer Engineering Department 17, <www.researchgate.net/publication/355576423_Blockchain_and_cyber_security> accessed on 11/10/2022

[22]Zoe Bernard, 'Everything You Need to Know About Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of Its Creator' (*Business Insider*, 2 December 2017) <https://www.businessinsider.in/tech/everything-you-need-to-know-about-bitcoin-its-mysterious-origins-and-the-many-alleged-identities-of-its-creator/articleshow/61895890.cms> (last viewed on 11/10/22)

A blockchain is simply a public ledger of all executed transactions or other digital events that have been shared among the users. The consensus of a majority of the system's users verifies each transaction on the Public Ledger. And once entered it is impossible to erase the information, a certain and variable record of every transaction is kept on the blockchain. Using a basic analogy, it is easier to steal a cookie from a cookie jar that is kept in a private setting than it is to steal it from a marketplace cookie jar where 1000 people are onlookers.

The most well-knownexample of blockchain technology that is directly related to a currencyis Bitcoin. It is also the most content IAS since it contributes to the development of fan unregulated, multibillion-dollar, in worldwide market for anonymous trade.

What makes Blockchain Secure?

Blockchain technology describes a decentralized database system with digital asset blocks that are cryptographically linked together. Blockchain technology describes a 'peer-to-peer' network database governed by a decentralized system.

It symbolizes a progression away from conventional agents and towards ethical behaviour.

Blockchain technology has been modified in every sector of dimensions, notably how firms conduct their daily operations. Integration of blockchain technology into corporate solution also eliminates the need for intermediaries in a number of essential services and reduce overheads[23].

The SecurityArchitecture of Blockchain Technology

The blockchain records are secured via cryptography,where each network user has their own private and secure keys. This key serves as a unique digital signature and is assigned straight to the transaction keys. Blockchainprotects against hostile attacks forbids them, and encrypts form data to make it secure.

With the use of high tech, enterprisessegregated their rights and duties. It safeguards confidential data without compromising privileged user access with aid assistance.

Every layer of blockchain technology is empowering for creating enterprise applications.

[23]Mayank Sahu, 'What Makes Blockchain Secure: Key Characteristics & Security Architecture | upGrad Blog' (*upGrad blog*, 8 January 2021) <https://www.upgrad.com/blog/what-makes-blockchain-secure/>accessed on 11/10/2022

The following components are among these layers:

- Operator access layers
- The presentation layers
- Layers for managing identities and access
- The requisition layers
- The web layers
- The infrastructure or foundation layers.

Blockchain is specially made to be profitable over time.Blockchainprofessionals can assist us in putting the necessary safeguard in place to ensure the success of fewer blockchain solutions.Blockchains' highly encrypted,irreversible data blocks provided us with the ability to combat any fraud. High-grade security requirements are used by blockchain technology to protect the encryption keys as well[24].

Key Attributes of the Blockchain Security

The block hash value connected a link between each block in the blockchain and the one before it.This makes the blockchain more resistant to manipulation Since in order to evade detectionHacker would have to alter both the block holding the original transaction and any blocks connected to it.

The blockchain is made to be safe, unchangeable and impenetrable. The following features are:

- Decentralization.
- Cryptography and Hashing
- Consensus protocol

Decentralization: Blockchain operates on a decentralized network where information hasbeen shared andupdated to all participants consistently in little bits.Hence eachblockcarries the updated information.All participants will validate any changes before they are accepted and only then will they be added to the blockchain. Decentralization hence prevents a single point of failure while allowing for a single version of the truth.

[24]*Ibid* accessed on 11/10/2022.

Cryptography and hashing: Preventing cyber-attacksthe complex mathematical algorithm safeguards the data. Each transaction is hashed using cryptography, and the block contains all the transactions. In order to create a new value, known as a hash digest,hashing takes an input value and applies hashing algorithm(SHA-256 in the case of Bitcoin). Depending on the algorithm the digest has a predetermined length.It is hard to estimate the value of the digestbecause even a small change in the value causes the digest to alter totally and in an unforeseen way.Now the previous blocks block's blockhashand this one of the transactions are combined to create a new block hash,which is then Put in the block header.This is how a chain of blocks is created using a cryptographically secure hash function.

Consensus Protocol: A simple majority of network users must be conquered in order for a transaction to be valid in accordance with the consensus protocol. The transaction is verified by a single miner, but the entire network can verify the veracity of the validator but examine the "proof-of-work".

As a result, even if there are a few malevolent Users on the network, they are quickly weeded out and their opinion never takes into consideration.

The three pillars of security that make up blockchain integration and deter any sort of wrongdoing are these key characteristics[25].

Blockchain tech is the Future

Blockchain has come a long way from its original conception as a platform for Bitcoin in 2009 by 'Satoshi Nakamoto, to become technology to provide value to enterprises across sectors, far beyond the initially envisioned cryptocurrency arena.

China, the USA, Brazil, Chile, Canada, Singapore, and Switzerland are just a few nations that have already made significant strides in the blockchain industry.

In the future, technology is a tipping point in the coming days. Gartner's analysis claims that many new, creative businesses will make use of it and that at least one would be worth $10 billion by 2022 if it were used to build a company. For 30% of the world's consumers by 2030, it might serve as a foundational technology.

[25]Ankur Goyal, 'Blockchain Security: Is Blockchain Really Secure | Edureka' (*Edureka. co*, 21 November 2022) <www.edureka.co/blog/blockchain-security/#:~:text=Each%20block%20in%20the%20blockchain,to%20it,%20to%20avoid%20exposure%20(Last >. (Last viewed on 11/10/2022)

Blockchain will add corporate value that will increase to over $176 billion by 2025. By 2030, this would have further increased to $3.1 trillion. It merely illustrates the possibilities as it grows.

Digital certificate management, the pharmaceutical supply chain, transfers of land records, e-notary solutions, duty payment, automated customs enforcement and compliances, cryptocurrency wallets, records of healthcare, cross-border transportation, public service delivery, and charitable giving, are just a few of them. Data stored in blockchain technology is nearly infeasible to be hindered with, the credence and incumbency of e-government will be maintained.

The suggested policy initiative clearly outlines the objectives and effectively captures the potential. The system will provide an effective ledger storage method in a distributed setting by decentralizing, monitoring, time stamping, and immutably storing data[26].

Key Features of the Blockchain

- Shared ledger that is distributed.
- Enduring records.
- Distributed consensus mechanism.
- Smart contracting.
- Pairs of cryptography.
- Managing identities and access.
- Enhanced Security.
- Peer-to-Peer networks.
- Traceability and Transparency in business dealings.
- No requirement for engagement from a centralized authority or a reliable third party[27].

Cyber-attacks- Future of Cybercrime and Malware

[26]The Hindu Bussinessline, 'Blockchain Tech Is the Future' (*www.thehindubusinessline.com*, 20 December 2021) <www.thehindubusinessline.com/opinion/blockchain-tech-is-the-future/article37999487.ece>, accessed on 11/10/2022.
[27]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 11/10/2022

Any well-positioned firm might be destroyed by a successful cyberattack. Security breaches are the main reason victim firms get a terrible reputation, victim firms get a terrible reputation, in addition to resulting in huge financial losses.

Companies that deal with the data of the consumers like Equifax and USCB America need an adequate level of Cyber Security. Businesses that use digital network services are facing a lot of difficulties and challenges right now. Online activities continue to be plagued by more advanced and harmful cyberattacks and hacks. A growing number of significant IT firms, like LG, Microsoft, Yahoo, Facebook, and Siemens, to name a few, are also becoming targets as this scenario worsens.

Today, corporations must contend with ransomware attacks and some other types of data breaches on a daily basis. Recent research and data show that even sacred state institutions like presidential elections aren't immune to these threats. This demonstrates that governments as well as other entities are now concerned about cybersecurity in addition to businesses. Analysing current trends and data in cyberattacks is advisable for the creation of effective cybersecurity defence methods[28].

- Over $75 billion is lost to businesses each year due to ransomware.
- Email is used to distribute malware over 90% of.
- Every day, around 200,000 new malware strains are created. With time, this number is anticipated to increase.
- 34% of the organisations that were infected by malware needed a week or so to restore data access.
- By2023, the US will account for 50% of all worldwide data breaches.
- The majority of small firms believe they are "unlikely" to experience cyberattacks[29].

The Million Dollar Cyber Heist

To conduct international transactions and transfer funds internationally, banks utilise standard electronic communications composed of codes and IDs, sort of a universal financial language. After having established methods for adhering to legal standards by verifying the

[28]Julien Legrand, 'The Future Use Cases of Blockchain for Cybersecurity' (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity>. Accessed on 11-10-2022.
[29]PurpleSec, '2023 Cyber Security Statistics Trends & Data' (*PurpleSec.us*) <https://purplesec.us/resources/cyber-security-statistics/>.accessed on 11-10-2022.

participants, finding abnormalities and keeping an eye out for anything that seems suspicious or abnormal. However, even having all of the strong financial defences in place with legions of back-office employees keeping an eye on money transfers, hackers occasionally succeed in escaping with very significant monetary amounts. A large theft occurred. The national bank of the nation, Bangladesh Bank, has an account with the New York Federal Reserve, and a hacker stole about $81 million[30].

The bold scheme called for stealing an enormous $1 billion from such an account, however, the NY Fed has been vital to block the majority of the theft thanks in large part to some unanticipated good fortune[31].

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial platform serves as the brain of the global banking system, according to experts of BAE Systems, a defence contractor located in the United Kingdom. The bank-owned organisation SWIFT, which is in charge of communication protocols, the requisite hardware and software as well as the supervision of the overall secure network, is also facing criticism. For almost 10,000 banks and businesses, the network processes 25 million transactions daily. Critics claim that SWIFT hasn't improved the security situation surrounding its network enough over the years. If SWIFT wanted to ensure that communications across its network were secure, it should have made investments in cutting-edge technology.

The Bangladesh hack was carried out by competent thieves who were familiar with the system. They avoided the best defences and instead targeted the international payments network's weakest connections.

Financial companies would be irresponsible if they did not take blockchain-based technologies into consideration, given the gravity of the Bangladesh incident. Therefore, banks are increasingly looking to blockchain seeking assistance and researching hybrid systems, which promote and sustain a distributed ledger system while having a single authority manage information centrally[32]. The possibilities for using blockchain technology in cyber security are practically infinite. The application of blockchain technology to combat

[30]Editorial Team, 'Can Blockchain Prevent Cybercrime?' (*Finextra Research*, 31 August 2016) <www.finextra.com/blogposting/13032/can-blockchain-prevent-cybercrime>, accessed on 11-10-2022
[31]*Ibid* accessed on 11-10-2022
[32]Rebecca Campbell, 'Is Blockchain the Answer to Preventing Cybercrime?' (*CCN.com*, 4 March 2021) <www.ccn.com/blockchain-cybercrime-prevention>. accessed on 12-10-2022)

cybercrime might be extended to the banking system, legal, real estate, and any other sector that needs third-party verification[33].

The Future of Cyber-attacks & Malware

The present, rapid growth in technology thus provides a breeding ground for cyberattacks, allowing them to develop and become more effective. Hackers will undoubtedly have additional possibilities once fifth-generation (5G) networks, which provide 10 times faster download rates than current networks, go live. A greater likelihood of greater cyberattacks and also hacking of even more devices will result from faster speeds[34].

In 2022, it is anticipated that 14.4 billion Internet of Things (IoT) devices will be worldwide connected[35]. Due to the enormous economic need for IoT, businesses are developing a variety of applications, including wearable technology and smart homes. Security flaws might be disclosed by criminals if they are there.

Implementation of Blockchain in Cyber Security.

Blockchain has developed into one of the finest secure ways to conduct transactions in the globe of digital networks, while not being completely impenetrable. The Technology has received accolades for preserving data integrity mostly in the way it was intended and constructed. It might be beneficial to many industries if used properly. Blockchain technology has the ability to be used in a wide variety of applications. Utilizing its integrity guarantee to provide cybersecurity remedies for several other technologies would be among its finest uses[36].

Here are a few examples of how blockchain potentially be utilised going forward to improve cybersecurity

[33]Data Privacy Philippines, 'Blockchain Technology in the Fight Against Cybercrime' (*privacy.com.ph*) <www.privacy.com.ph/blockchain-technology-in-the-fight-against-cybercrime/>, accessed on 12-10-2022
[34]Surajeep Singh, 'Potential Use Cases of Blockchain Technology for Cybersecurity | ITBE' (*IT Business Edge*, 16 July 2021) <www.itbusinessedge.com/security/potential-use-cases-of-blockchain-technology-for-cybersecurity/> accessed 11 October 2022.
[35]Mohammad Hasan, 'State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally' (*IoT Analytics*, 18 May 2022) <https://iot-analytics.com/number-connected-iot-devices/#:~:text=In%202022,%20the%20market%20for,27%20billion%20connected%20IoT%20devices.> accessed 11 October 2022.
[36]Julien Legrand, 'The Future Use Cases of Blockchain for Cybersecurity' (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity> accessed 11 October 2022.

1. Securing Private Messaging:

With each new day, more social applications are released as social commerce becomes more popular. During these exchanges, enormous volumesof metadata were collected. The majority of social networking site customers employ flimsy, weak passwords to safeguard their services and personal data.

Numerous cyberattackshave previously been performed against these social media sites notably Facebook and Instagram in the near past. The majority of messaging firms are beginning to accept blockchain as a more secure alternative towards Encryption that end-to-end companies presently employ for protecting user data. A standardised security protocol may be established using blockchain technology. Blockchain could be used to provide a single API architecture for providing cross-messenger communications infrastructure.

Due to these cyberattacks, potentially millions of profiles were compromised, exposing user data to unauthorized parties. If properly integrated into these communications systems, blockchain technology might shield against such assaults in the future.

2. IoT Security:

Thermostats and WIFI routers are examples of edge devices that hackers are increasingly using to access larger networks. Due to the current preoccupation with “artificial intelligence (AI)”, hackers now have an easier time breaking into edge gadgets such as "smart" switches and gaining access to larger mechanisms such as home automation. The majority of these IoT gadgets have poor security features.

In this situation, by decentralising its management, blockchain may be utilised to safeguard such large-scale systems or gadgets. The strategy will allow the gadget to independently decide on security measures. By identifying and responding to questionable instructions from unfamiliar networks, edge devices become more protected by not relying on the centralized admin or authorities. Typically, hackers access a device's central control and instantly seize total control of both the systems and devices[37]. A significant use case to sustain information security throughout the IoT system uses blockchain technology to increase security by

[37]Julien Legrand, ‘The Future Use Cases of Blockchain for Cybersecurity’ (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity> accessed 12 October 2022.

utilising device-to-device encrypting to network security, data handling mechanisms, and authentication[38].

3. DNS & DDoS Security:

When it comes to connecting domain names and IP addresses, the "Domain Name System (DNS)" is comparable to a community database.DNS is highly centralised, which makes it an ideal target for intruders who compromise the relationship between both IP addresses and a website's name[39]. The DNS may be kept with increased security because of the irreversibility and decentralised nature of blockchain technology[40].

"Distributed Denial of Service (DDoS)" assaults are amongst the most common types of cyberattacks nowadays, when criminals try to interrupt service delivery by flooding the Internet with traffic. These cyberattacks cause the resource services to malfunction or slow operations[41]. Blockchain has shown to be a successful defence against these assaults thanks to its immutability and cryptographic features[42].

4. Decentralization Medium of Storage:

Organizations are increasingly concerned about business data theft and hacking. The majority of businesses continue to adopt the centralised way of storing data. A hacker has to target just one weak spot in these systems in order to gain access to all the data that is kept there.

Decentralized storage is made possible with the use of blockchain technology, preserving digital data. By using this mitigation technique, hackers would find it more difficult or perhaps impossible to access database storage systems. An organisation which has already

[38]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 12/10/2022
[39]Julien Legrand, 'The Future Use Cases of Blockchain for Cybersecurity' (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity> accessed 12 October 2022.
[40]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 12/10/2022
[41]Julien Legrand, 'The Future Use Cases of Blockchain for Cybersecurity' (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity> accessed 12 October 2022.
[42]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 12/10/2022

integrated blockchain technology into its operations is "Apollo Currency Team (The Apollo Data Cloud)[43]".

5. The Provenance of Computer Software:

Blockchain may be utilized to verify the accuracy of software installation and thwart outside interference. Utilizing blockchain technology validates actions, like firmware upgrades, patches and installers, to block the introduction of malignant software onto computers, similar to how MD5 hashes are used. When using MD5, vendor websites' hashes are matched to the new software's identification. This approach is not totally secure since the hashes that are accessible on the network of the supplier could already be tampered with. Distributed ledger technology, whereas irrevocably stores the hashes within that blockchain. The data which are a record kept on the blockchain are irrevocable. By comparing the software's hashes to those on the blockchain, the blockchain may thus be more effective in confirming the software's integrity[44].

6.Maintaining Data Transmission Safe:

Future data transmissions might be protected against unlawful access via blockchain technology. Data transmission may be safeguarded to prevent hostile actors from accessing it, whether they are an independent person or a group, by using the technology's full encryption capability. This strategy would result in a broad rise in trust and data integrity sent over the blockchain. Hackers with malevolent intentions intercept transmitted data and change or remove it. This creates a significant vacuum for ineffective channels of interaction like emails.

7. Infrastructure Verification for Cyber-Physical Systems:

Information created by cyber-physical systems has suffered from data manipulation, system configuration issues, and system failures. To validate the state of any cyber-physical infrastructure, however, one might use blockchain technology's capabilities for data integrity and authentication. Blockchain-generated data about infrastructure's parts can provide better assurance for the full custody chain.

[43]Doug Drinkwater, '6 Use Cases for Blockchain in Security' (*CSO Online*, 18 February 2018) <www.csoonline.com/article/3252213/6-use-cases-for-blockchain-in-security.html> accessed 12 October 2022.

[44]*Ibid*accessed on 12/10/2022.

8.Minimize the threat to human safety posed by cyberattacks:

Public and unmanned military equipment transit have lately been introduced because of creative technical breakthroughs. The Internet, which enables the flow of information collected by the sensors to distant location databases, is responsible for making such driverless vehicles and warheads conceivable. But cybercriminals have been working to crack and access systems like the "Car Area Network (CAN)". Once those networks are breached, hackers have full control over essential automobile systems. All these situations would directly affect people's safety. However, a lot of problems might be avoided if data entering and leaving such systems were verified on the blockchain[45].

Real-life application of the Blockchain

Let us look into some real-life implementations of Blockchain and understand how companies and industries are applying blockchain technology.

1. Barclays (London, England), Traditional Banking:

To improve the security of financial transactions, Barclays has applied for a patent on the usage of blockchain. Using distributed ledger technology, it seeks to stabilise Bitcoin transactions (DLT). Blockchain enables the bank to securely keep consumer data[46].

2. CISCO (San Jose, California), IoT:

Due to ledger technology's ability to eliminate single points of failure and the benefits of encryption, Cisco intends to employ blockchain to protect IoT devices. The networking behemoth Cisco is a member of the 'Trusted IoT Alliance, an organization that is looking at scaling technology to improve the security of IoT goods.

3. Coinbase (San Francisco, California), Cryptocurrencies:

[45]K Gagandeep, *Scalability in Blockchain: Challenges and Solutions in Handbook of Research on Blockchain Technology* (Academic Press) 373-406, accessed on 12/10/2022.

[46]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 13/10/2022

Users can purchase and sell virtual currencies on Coinbase. Wallets and passwords are kept secure in a database by Coinbase using encryption. It also conducts background investigations on workers to guarantee the security of their cryptocurrency.

4. Australian Government (Canberra, Australia)

One of the global pioneers in implementing governmental blockchain is the Australian government. In order to protect the preservation of government records through the development of a blockchain ecosystem, the government has also teamed with IBM[47].

5. The State of Colorado (Denver, Colorado), Government:

In May 2018, the Colorado Senate approved a measure urging the government to take blockchain into account for data security and record preservation. According to reports, there are 6 to 8 million attempted assaults in Colorado every day, thus the state has every incentive to use blockchain's encryption techniques to safeguard its most important networks.

6. Chinese Military (Beijing, China), Defense and Military

The Chinese military and government are working on using blockchain technology to protect sensitive military and government data.

7. J. P. Morgan (New York, NY), Traditional Banking:

The largest banking institution in the US, JPMorgan Chase, has created Quorum, a corporation implementing Ethereum. The system processes private transactions using blockchain technology. The bank implements visible yet cryptographic algorithm transactions using smart contracts mostly on the Quorum network.

8. Santander Bank:

The very first bank in the UK to use blockchain was Santander, which used it to securitize its payment services business. Customers may safely transfer money across Santander wallets in Europe and Latin America.

9. Health Linkages (Mountain View, California):

[47]Sam Daley, '20 Blockchain in Cybersecurity Examples' (*Built In.com*, 16 September 2022) <https://builtin.com/blockchain/blockchain-cybersecurity-uses> accessed 13 October 2022.

They want to utilise Blockchain to protect patient records, limiting access to them to certain staff members. Additionally, it will be utilised to maintain a sequential track of significant medical occurrences, which will aid clinicians in their decision-making.

10. Lockheed Martin:

The first American defence contractor the adoption of blockchain technology system is Lockheed Martin. As a way to incorporate blockchain cybersecurity strategy features throughout the system architectures, supply chain risk control, and software development, the organisation partnered up with Guard time Federal[48].

We've compiled ten businesses that employ blockchain as a weapon system in the battle to safeguard our most private data since its application in cybersecurity is pervasive.

Potential Challenges for Blockchain to mainstream adoption.

Although blockchain has lots of use cases we cannot disregard the numerous difficulties.

The main issue is scalability because numerous variables affect how quickly transactions are processed at the moment[49]. Checking the network's scalability is crucial since blockchain networks feature fixed block volumes and transaction restrictions. Companies may encounter challenges since adopting Blockchain technology necessitates a whole overhaul of the existing systems[50].

Interoperability is another problematic issue since it is still in its infancy in the nation and more work has to be undertaken in several crucial areas. The localization of data is a topic that requires attention and study[51].

[48] *Ibid* accessed on 13/10/2022.
[49] The Hindu Bussinessline, 'Blockchain Tech Is the Future' (*www.thehindubusinessline.com*, 20 December 2021) <www.thehindubusinessline.com/opinion/blockchain-tech-is-the-future/article37999487.ece>, accessed on 13-10-2022.
[50] Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 13/10/2022
[51] The Hindu Bussinessline, 'Blockchain Tech Is the Future' (*www.thehindubusinessline.com*, 20 December 2021) <www.thehindubusinessline.com/opinion/blockchain-tech-is-the-future/article37999487.ece>, accessed on 13-10-2022.

Learning Blockchain technology requires in-depth familiarity with several developing, coding, and other tools. As a result, there aren't enough Blockchain developers accessible right now, despite the fact that blockchain technology has numerous uses[52].

Conclusion

Accepting the fact that cybercrime is lucrative and constantly changing is vital. Therefore, no cyber defence system can be said to be completely secure.

Ever a cybersecurity system that is currently thought to be the most effective can use that efficiency in the future. However, at this time, when every organization wants to implement a cybersecurity solution that is safe, vigilant, and Resilient, Blockchain has a lot to offer. Stronger technical infrastructure can be built to safeguard enterprises from cyberattacks using blockchain-powered cybersecurity controls and standards. Along with Blockchain, this may also call for the integration of AI, IoT and ML three more profound technologies.

This paper identified the recent studies that are available on how blockchain technology can affect cyber-security. This paper solely focused on cyber-security. Application for blockchain in cyber security has developed and strengthened the current initiatives to improve security and deter malicious actors.

Without a doubt, blockchain tech is progressive and something that will bring a major difference in how people conduct business. Having said that, there are still a few kinks that need to be worked out before we can utilise the technology to its fullest extent. In the interim, while using the technology, you must take precautions to keep yourself safe. You must be careful not to divulge any personal information online or to allow others to cusses your IP address or browser history. You can ensure that no hackers can access your cryptocurrency wallet or any other sensitive data by using VPNto hide your IP address.

BIBLIOGRAPHY

- Acharjee S, *The History of Cybercrime: A Comprehensive Guide(2021)* (2021)
- Bernard Z, 'Everything You Need to Know About Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of Its Creator' (*Business Insider*, 2 December 2017)

[52]Nandini Dey, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>, accessed on 13/10/2022

<www.businessinsider.in/tech/everything-you-need-to-know-about-bitcoin-its-mysterious-origins-and-the-many-alleged-identities-of-its-creator/articleshow/61895890.cms>.

- Bsigroup.com, 'Cyber Security - Protecting Networks, Computers and Data' (*https://www.bsigroup.com/en-GB/*) <www.bsigroup.com/en-GB/Cyber-Security/>.
- Campbell R, 'Is Blockchain the Answer to Preventing Cybercrime?' (*CCN.com*, 4 March 2021) <www.ccn.com/blockchain-cybercrime-prevention>.
- Chaubey PR, *"An Introduction to Cyber Crime and Cyber Law"* (Kamal Law House 2021).
- Cyber laws and Information Security Advisors., '11-ways-to-protect-yourself-against-cybercrime' (*https://www.cyberralegalservices.com/*).
- Daley S, '20 Blockchain in Cybersecurity Examples' (*Built In.com*, 16 September 2022) <https://builtin.com/blockchain/blockchain-cybersecurity-uses> accessed 13 October 2022.
- Data Privacy Philippines, 'Blockchain Technology in the Fight Against Cybercrime' (*privacy.com.ph*) <www.privacy.com.ph/blockchain-technology-in-the-fight-against-cybercrime/>.
- Dey N, 'Role of Blockchain in Cybersecurity - GeeksforGeeks' (*GeeksforGeeks*, 22 September 2021) <www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/>.
- Drinkwater D, '6 Use Cases for Blockchain in Security' (*CSO Online*, 18 February 2018) <www.csoonline.com/article/3252213/6-use-cases-for-blockchain-in-security.html> accessed 12 October 2022.
- Fatima DT, *Cyber Crimes* (Eastern Book Company 2021).
- Gagandeep K, *Scalability in Blockchain: Challenges and Solutions in Handbook of Research on Blockchain Technology* (Academic Press).
- Goyal A, 'Blockchain Security: Is Blockchain Really Secure | Edureka' (*Edureka.co*, 21 November 2022) <www.edureka.co/blog/blockchain-security/#:~:text=Each%20block%20in%20the%20blockchain,to%20it,%20to%20avoid%20exposure%20(Last>.
- Hasan M, 'State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally' (*IoT Analytics*, 18 May 2022) <https://iot-analytics.com/number-connected-iot-

devices/#:~:text=In%202022,%20the%20market%20for,27%20billion%20connected%20IoT%20devices.>.

- JavaTpoint.com, 'What Is Cyber Security? Definition, Types and Importance - Javatpoint' (*www.javatpoint.com*) <www.javatpoint.com/what-is-cyber-security>.
- Legrand J, 'The Future Use Cases of Blockchain for Cybersecurity' (*cm-alliance.com*, 4 September 2020) <www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity>.
- McAfee and CSIS Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact, *Press Release | McAfee and CSIS Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact.* (2020) <www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629>.
- Mclean M, '2023 Must-Know Cyber Attack Statistics and Trends.' (*Embroker.com*) <www.embroker.com/blog/cyber-attack-statistics/>.
- Muskan, 'What Is Cybercrime? Different Types and Prevention' (*Intellipaat Blog*) <https://intellipaat.com/blog/what-is-cybercrime/>.
- National Agency for Information And Communication And Technology, 'Types of Cybercriminals' (*www.antic.cm*) <https://antic.cm/index.php/en/security/cybercriminality/222-cyber-criminality-types-of-cybercriminals.html>.
- Norwich University Online, 'Who Are Cyber Criminals?' (*https://online.norwich.edu/*, 13 February 2017) <https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals>.
- Obayes MQ, 'Blockchain and Cyber Security' [2021] Emam Reza University of Mashhad Faculty of Engineering Copmputer Engineering Department 17 <www.researchgate.net/publication/355576423_Blockchain_and_cyber_security>.
- Piscini E, Dalton D and Kehoe L, 'Blockchain & Cyber Security' Deloitte EMEA Grid Blockchain Lab 14.
- PurpleSec, '2023 Cyber Security Statistics Trends & Data' (*PurpleSec.us*) <https://purplesec.us/resources/cyber-security-statistics/>.
- Sahu M, 'What Makes Blockchain Secure: Key Characteristics & Security Architecture | upGrad Blog' (*upGrad blog*, 8 January 2021) <www.upgrad.com/blog/what-makes-blockchain-secure/>.

- Seemma P, Nandhini S and Sowmiya M, 'Overview of Cyber Security' (2018) Vol. 7(Issue 11) IJJRCCE 5.
- Singh S, 'Potential Use Cases of Blockchain Technology for Cybersecurity | ITBE' (*IT Business Edge*, 16 July 2021) <www.itbusinessedge.com/security/potential-use-cases-of-blockchain-technology-for-cybersecurity/>.
- Team E, 'Can Blockchain Prevent Cybercrime?' (*Finextra Research*, 31 August 2016) <www.finextra.com/blogposting/13032/can-blockchain-prevent-cybercrime>.
- The Hindu Bussinessline, 'Blockchain Tech Is the Future' (*www.thehindubusinessline.com*, 20 December 2021) <www.thehindubusinessline.com/opinion/blockchain-tech-is-the-future/article37999487.ece>.
- Upadhayay V, 'Cyber Crime in India' (*legalservicesindia.com*, 31 October 2021) <www.legalservicesindia.com/law/article/2266/6/Cyber-Crime-In-India?id=2266&u=6>.