*International Journal of Social Science and Economic Research*

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

# An in Depth Analysis on The Use of Cryptography and Security Systems To Prevent Cyber Crimes

Abhishek Gupta

Lotus Valley International School

DOI: 10.46609/IJSSER.2024.v09i07.012 URL: https://doi.org/10.46609/IJSSER.2024.v09i07.012

Received: 4 July 2024 / Accepted: 18 July 2024 / Published: 28 July 2024

## ABSTRACT

*The extent of cybercrime has grown exponentially with the development of technology. As the world has globalized, cybercrimes have increased especially in those countries, which have lax security systems. The only way out is to invest in cybercrime prevention technology by all stakeholders namely the government, companies, and individuals. The availability of bitcoins and Ethereum has made it easy for criminal proceeds to be collected and used for nefarious activities.*

**Keywords:** Cybercrime, Cybersecurity, Cryptography, Hacker, technology, security, data, digital, encryption, social, economic, organizations.

**Research Question:** An attempt will be made to analyze the reasons for increased cyber crimes in the world today. What are the reasons for a sudden surge in such crimes? What is the extent to which cyber thieves have used technology to commit these types of thefts? What are the areas that they work on? Are the proceeds moving towards finance, smuggling, terrorism, and drugs? What are the reasons that there has been a surge in such thefts? What are security systems in place that could prevent these crimes from being committed? These and similar types of questions will be attempted to be answered in the course of the paper.

## 1. Introduction

Cyber Crime is wreaking havoc on the global economy, national security, social stability, and individual interest. Crime integrates the social, economic, political, and technological as well as cybersecurity factors in an economy. Cybercrime is a broad term used by government, businesses, and the general public to account for various criminal activities and harmful behavior involving the adoption of computers, the internet, or other forms of information communication technology (ICTs) (Wall, 2007). As an emerging social phenomenon in the information age,

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

cybercrime has aroused growing concern around the world due to its high destructiveness and widespread influence. With the rapid development of ICTs and the increasing prevalence of the internet, these criminal activities are significantly disrupting the global economy, national security, social stability, and individual interest.

Cybercrime is extremely complicated in nature and involves many disciplines that include:

- Criminology
- Computer Science
- Psychology
- Sociology
- Economics
- Geography
- Political Science
- Law

**Figure 1: Image of Cybercrime**


Source: https://datacyper.com/cyber-crime-causes-and-preventive-measures/

This concept encompasses a wide range of criminal activities that are carried out using digital devices and/or digital networks. These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams, and other malicious acts. It is also the use of a computer as an instrument to further illegal ends that include committing fraud, trafficking in child pornography, violating privacy, and hacking online business-related activities.

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

## 2. History of Cybercrime

The model history of cybercrime began when Allen Scherr (1962) launched a cyberattack against the MIT computer networks, stealing passwords from their database. Technically, the first cyberattack happened in France well before the internet was even invented in 1834, attackers stole financial market information by accessing the French telegraph system. It is from that time onwards that cybercrime has grown exponentially, marked by an intriguing evolution of tactics, techniques, and procedures – all of these being implemented for malicious gain.

Cybercrime did not find its footing till the middle of the 20th century, spurred by the digital revolution, cybercriminals used this technology to engineer new, devious ways to part people and organizations from their data and money.

In 1971, the first computer virus was created for research purposes by Bob Thomas at BBN Technologies, it was referred to as the ‘Creeper virus’.

In 1981, Ian Murphy became the first person to be convicted for committing a cybercrime after successfully hacking into AT&T's internal system and changing their computer's clocks causing immense havoc to their systems.

In 1988, the first major cyberattack on the internet came from a Cornell graduate student Robert Morris under the name of ‘Morris Worm’, whose domain was academic researcher. This affected computer systems at Stanford, Princeton, John Hopkins, and NASA, to name a few.

In the 1990s, the internet-connected people across different communication networks wherever they were, all over the world. As new technologies developed, trust and safety controls were not a major concern. The main aim of this industry was to create groundbreaking applications for communication and business efficiency. It was at this time that the underground economy was growing in strength. The impact of this economy was so vast that in 1994 a 16-year-old British schoolboy and his accomplice used a 'Password sniffer' program that crippled the Air Force's Rome laboratory while stealing research data used as attack instructions for warplanes in battle.

In 1995 V. Levin, attempted to rob a bank. He hacked into City Bank's network and conducted fraudulent transactions worth more than 10 million dollars and transferred into various bank accounts worldwide.

Kevin Mitnick was the first person to penetrate large networks by manipulating people and using insiders to get the codes access into Motorola and Nokia.

In 1999, a computer virus under the name ‘Melissa’ affected users across the internet corrupting Microsoft document files.

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

The decade of the 2000s saw a number of sophisticated attacks and an abundance of advanced persistent threats (APTs), which were sponsored by nation-states that caused significant damage to critical sectors of the global and digital economy.

There was an explosion of cyberattacks in the decade of 2010. This transformed cybercrime into a profitable industry. Trillions of dollars were lost as bushwhackers developed increasingly sophisticated programs targeting organizations of all sizes. The notable crimes of this period were:

- Sony PlayStation network breach compromised information of 77 million users.
- Equifax data breach compromising 147 million people.

The decade of 2020s seems to be one where bushwhackers would continue to exploit vulnerabilities in inter-connected systems, compromising critical infrastructure and extorting organizations through ransomware attacks.

**Figure 2: Cyber Attackers**


Source: https://data-flair.training

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

**Figure 3: Revenue lost due to Cybercrime**


Source: https://www.zimlon.com

## 3. Definition

To understand the impact that cybercrime and cryptography have on the world today, it is important to define these words to realize their impact on the increasingly digital world.

### 3.1. Cybercrime

This is defined as a crime in which a computer is the object of the crime (Hacking, Phishing, and Spamming) or is used as a tool to commit an offense (Child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, and business trade secrets or use the internet for exploitive or malicious purposes. These criminals can use computers for communication, documentation, and/or data storage. These crimes involve identity theft, data breaches, computer viruses, scams, and other malicious acts. Cybercriminals exploit *vulnerabilities* in computer systems and networks to gain unauthorized access, steal sensitive information, and disrupt services that cause financial and regulatory harm to individuals, organizations and government.

The World Economic Forum's 2023 Global Risk Report ranks cybercrime as one of the top ten risks facing the world today. If the extent of cybercrime was equated to an economy, then it

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

would count as the third-largest economy in the world (Freeze, Di, 2023, Cybercrime Magazine). In terms of numbers it is predicted to cause over $9 trillion in damages worldwide in 2024 (Freeze, Di, 2023, Cybercrime Magazine).

### 3.2. Cryptography

Cryptography is the communication in the presence of adversaries. It is an art and sciencethat is referred exclusively to encryption which is the process of converting ordinary information (Plaintext) into unintelligible gibberish (Cipher text). It provides methods that enable a communicating party to develop trust that his communication has the desired properties.

The desired properties could include:

- Privacy
- Authentication – The recipient of a message convinces himself that the message originated from the alleged sender.
- Signatures – The recipient of a message convinces the third party that the message received has the alleged sign up.
- Minimality – What is communicated is what is specifically desired.
- Simultaneous exchange – Something of value is not released until something of value is received.
- Coordination – In multiparty communications all of them coordinate towards a common goal.

There are different types of encryptions. Key based encryption algorithm can either be symmetric or asymmetric. Asymmetric is known as Public Key encryption. In the former, a common key is used and the same cryptographic algorithm is used to scramble and unscramble the message. The most widely used symmetric encryption is the Triple Data Encryption Standard (3DES). The problem with this system is that a single key has to be shared in pairs of each sender and receiver. In a distributed environment with large number of combination pairs involved it becomes difficult for one recipient to keep so many keys in order to support all communications.

*Public Key Encryption* is known as asymmetric encryption that uses two different keys, a public key known by all and a private key known by only the sender and the receiver. The one that is known to the sender and receiver is a closely guarded one, this ensures data confidentiality. For

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

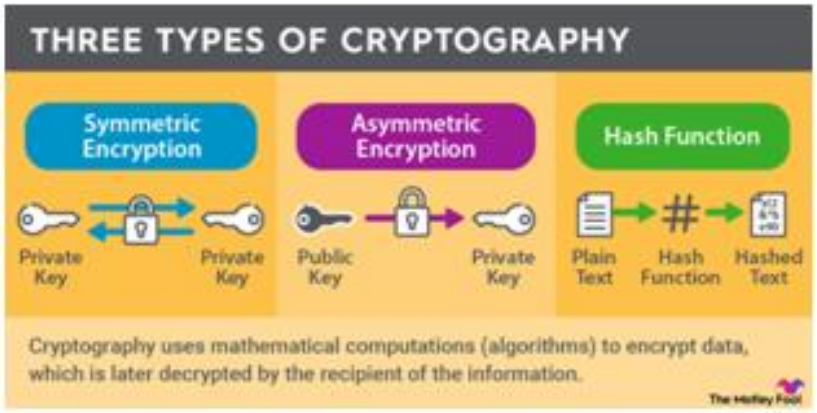
the data to be modified by an attacker it requires the recipient's private key. The algorithms for public key encryption include RSA, DSA, PGP, and EL Gamel. The biggest problem with public key encryption is the speed as this involves exponentiation of very large numbers which in turn take longer to compute. They have a potential to suffer from 'the man in the middle attack', which implies that an attacker sniffs packets of a communication channel, modifies them and inserts them back onto the channel.

*Hashfunction* is a computational method that can map an indeterminate size of data into a fix size of data. It plays a crucial role in various applications such as data storage, retrieval, and cryptography. It is a function that takes an input or message and returns a fixed size string of bytes. The output typically a number is called the *Hash code* or *Hash value*, the main function being to efficiently map data of arbitrary size to fix size value.

The key properties of Hash functions are:

- Deterministic
- Fixed output size
- Efficiency
- Uniformity
- Pre-image resistance (unfeasible to reverse the Hash function)
- Collision resistance (difficult to find two different inputs that produce the same Hash value.)
- Avalanche effect (a small change in the input should produce a significantly different Hash value.)

**Figure 4 – Cryptography**




Source – www.fool.com

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

**Applications of Hash Functions:**

- Hash tables
- Data integrity
- Cryptography
- Data structures

**Types of Hash Functions:**

- Division method
- Multiplication method
- Mid-square method
- Folding method
- Cryptographic Hash functions
- Universal Hashing
- Perfect Hashing

Cryptographic Hash functions are designed to secure and are used in Cryptography. The main examples are MD5, SHA-1, and SHA-256. The characteristics are that they are pre-image resistance, second pre-image resistance, and collision resistance. The advantages being that they are of high security, and disadvantages are that they are computationally intensive. This function is a versatile one in which cryptographic algorithm maps an input of any size to a unique output of fixed length of bits. The resulting output is known as a Hash digest, Hash value or Hash code, which is the resulting unique identifier. Specifically a Cryptographic Hash Function (CHF) is an equation that is used to verify the validity of the data. It has many applications, mainly, in information security.

**4. Areas in which Cybercrime have become rampant and why?**

Cyber-crime has become a big business industry in the last decade. This industry has its entire eco-system of criminal organization being run like a legitimate organization. It is so brazen that this industry has started taking out pop-up ads selling their products. Though the cybercrime industry has exploded in the last decade, the fact is that this is not a new kind of threat. Cyber-

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

crime has expanded into its own eco-system that is full of ‘leak sites’, ’attack vectors’ that compromise business e-mails. This has a global footprint that is costing organizations more and more every year to tackle.

**Figure – 5 – Cybercrime**


Source: www.apac-insider.com

The twelve most common types of cyberattacks are:

1. Malware – This is malicious software and is a program or code that is created with the intent to do harm to a computer from a network or server. It leverages software in a malicious way.

2. Denial – of – Service (DOS) – It is a targeted attack that floods the network with false request in order to disrupt business operations. Users are unable to perform routine and necessary tasks. This costs the organization time, money, and other resources to restore business operations.

3. Phishing – This uses social engineering techniques to entice a victim to share sensitive information such as passwords, bank account numbers etc.

4. Spoofing – A technique through which the criminal disguises themselves as a trusted source with the aim to target and access systems to steal information and extort money.

5. Identity Based Attacks – These are extremely hard to detect as the valid user’s credentials have been compromised and an adversary is masquerading as that user, becoming difficult to differentiate between the user and the hacker.

6. Code Injection Attacks – Here the attacker injects a malicious code into a vulnerable computer or network changing its course of action.

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

7. Supply Chain Attacks – This targets a trusted third party vendor that offers services or software vital to the supply chain.
8. Social Engineering Attacks – Here the attacker uses psychological tactics to manipulate people into taking a desired action.
9. Insider Threats – These are internal employees, current or former that pose danger to an organization as they have direct access to a company's network.
10. DNS Tunneling – This leverages Domain Name System (DNS) bypassing traditional security measures.
11. IOT Based Attacks – This targets an IOT device or network allowing the hacker to assume control of the device (computer, laptop, mobile phone, servers etc.)
12. AI Powered Attacks – As AI and technology improves, attackers leverage these tools to get access to various networks and steal information.

The reasons that cybercrime is growing and succeeding is because they are primarily targeting:

- People
- Cybercriminals do their homework as most of the attacks are well researched one giving them an extremely high success rate.
- Numbers game – E-mails and messages are cheap and easy to send in bulk and if they send in thousands they need a very small percentage of victims to be successful.

Cybercrime is a complex social phenomenon driven by the compound interactions of underlying socio-economic factors. Human and Social factors play a substantial role in the formation of cybercrime at agglomerations. Human factors that influence cybercrime are important and are a part of sociological and psychological studies. The reason why this area is studied is because of cyberbullying, online harassment, identity theft, online fraud, phishing etc. for which traditional criminological and psychological theories are necessary and important to understand victimization.

It has been discovered from the studies that criminal motivation can stem from age, gender, ethnicity, education, socio-economic status as well as situational factors like online activities, time spent online, risk exposure, deviant behaviors etc.

What has also been analyzed is that cybercrime is a highly geographical phenomenon on a macro level scale with some countries accounting for a disproportionate amount of cybercrime (Kigerl,

ISSN: 2455-8834

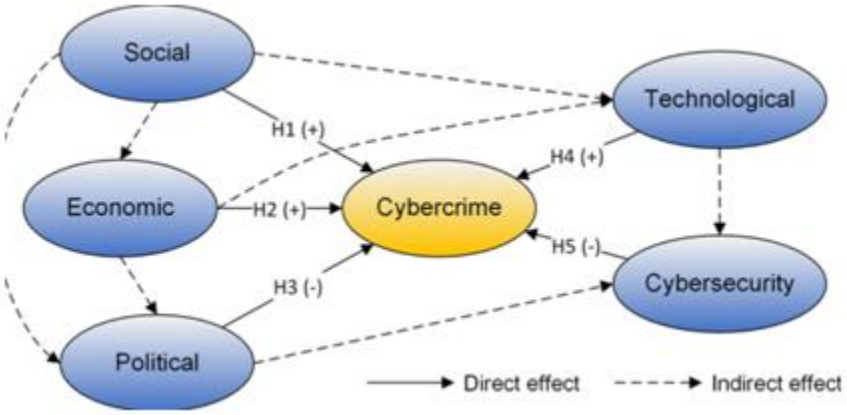
Volume:09, Issue:07 "July 2024"

2012). The special heterogeneity is further related to socio-economic context (Kshetri, 2010). Researcher like Carley (2014) found that Eastern European countries hosted a greater number of attacking computers due to their high level of computing infrastructure and corruption. Corruption played a major role in the level of the attack origination. The countries that were targeted were those with high GDP and better ICT.

The important driving forces of cybercrime are basically five inter-related components:

- Social
- Economic
- Political
- Technological
- Cybersecurity Factors

**Figure 6 – Five main reasons for increase in cybercrime**




Source: www.researchgate.net

With the increase in global urbanization as well as the information technology revolution, global connectivity has increased and along with it created unprecedented conditions and opportunities for cybercrime.

Motivations of cybercrime and illegal gains are poverty, unemployment, income inequality and other social disorders that are accompanied by social transformations leading to a culture of materialism. Developed economies that have superior ICT infrastructure provide convenient and low cost ambition for cybercriminals to commit crime. High educational attainment is another

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

factor associated with cybercrime, as this requires some level of computer skills and IT knowledge.

Influence of political factors is reflected in the regulation and intervention measures of governments in preventing and controlling cybercrime such as legal system, government deficiency, control of corruption and political stability. Corruption in law enforcement authorities make it hard for cybercriminals to be punished, while corruption in network operators or internet service providers make it easy for cybercriminals to apply for malicious domain names or register fake websites.

*Cybercrimes are typically attributed to political corruption, ineffective governance, institutional weakness, and weak rule of law.*

**5. Growth of Cryptography and Security Systems to handle these cybercrimes**

Sweden was the first country to make a law for data protection called 'Swedish Data Act of 1973'. It states that data must be protected against all unauthorized access. The USA was the second country to create a law to punish cyber criminality called 'Federal Computer System Protection Act of 1977'. Cybercrime constitutes illegal acts where a digital device or information system is either a tool or a target or a combination of both. Though the 'Hacker' term meaning has changed, the conceptualization of the activities of this group is seen as 'dark evil' whose intention is to cause damage against society's information system. There are some hackers whose online activities are perfectly legal. Hackers who commit crimes and cyber criminals accept the activity for a criminal motive.

Hackers can be categorized into:

- White Hats (They work within the law)
- Grey Hats (These are reformed black hats, but now working as security consultants)
- Black Hats (They are motivated by power, anger or hate. Their motive is to cause damage, steal information, and earn money.)

The different types of cybercrime are:

- Child Pornography
- Cyber Hate Speech
- Cyber offences against intellectual property
- Cyber Bullying
- Cyber Espionage
- Cyber Extortion

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

- Cyber Laundering
- Cyber Terrorism
- Cyber Theft
- Cyber Warfare
- Data Breach
- Disgruntled and former employees
- Hacking
- Identity Theft
- Online Gaming
- Online Obscenity
- Phishing
- Racism
- Religion Cyber Offences
- Revenge Porn
- Spam

Protection against cybercrime starts from taking personal measures for protection and then escalates to organizational, societal, Corporate, National, Military, and International levels. Technology by itself is not enough; it is the integration of fields like training, awareness, social aspects, culture, laws, prosecution, and International Corporation that are needed to blend with the technical situation to tackle cybercrime.

The technology that is applied to tackle cybercrime is the application *firewall* that secures files or data processing by specified software. A hardware measure to counteract cybercrime is a router that can save the IP-Addresses of a single computer system. The other counter measures include:

- Traditional Firewalls
- Programs or Algorithms for encryption or decryption
- Anti-Virus Programs
- Bio-metric Authentication Systems

The security systems that can be used are:

- Communication Security
- Cryptographic Security
- Emission Security
- Physical Security
- Transmission Security

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

- Security Information Security
- Network Security
- Operational Security
- Better End-User Education
- Development of Security Conscious Programming

**Major Security Problems.**

The major security problems are the following:

- Virus: A programs that one downloads without ones knowledge and it works against ones wishes.
- Worms: They do not need a host to hang on like a virus; it multiplies till it completely eats up all the current memory in the system.
- Hacker

**Figure 7: Best practices to overcome cybersecurity risks**


Source: tajassus.com

**6. The expense involved in using these new systems to prevent Cybercrime**

Certain news reports estimated the cost of prevention of cybercrime to be $600 billion a year. Senior vice president, James Lewis at CSIS (Center for Strategic and International Studies) has said ‘Cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding and the chances of being caught and punished are perceived to being too low’. The

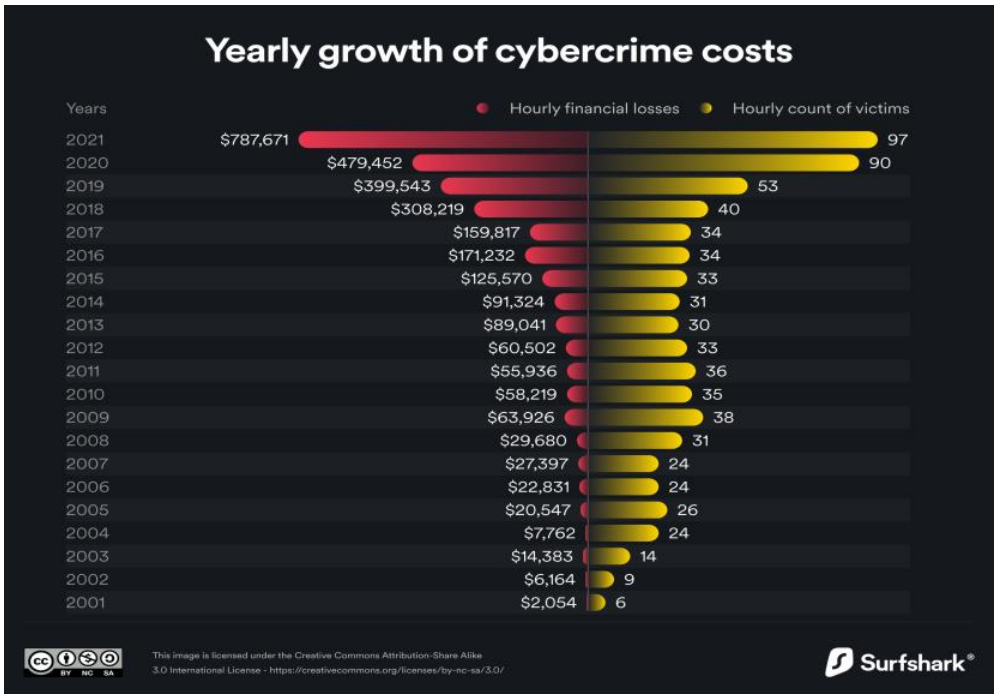
ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

preferred currency for cyber criminals is Bitcoins. They take advantage of the decentralized organization to conduct illicit transactions demanding payments from victims and further using the proceeds for criminal purposes. Block chain technology which is the bases in which bitcoins are based require no personally identifying information. Some estimates in 2023 indicated that the cost of cybercrime is estimated to top $8 million in 2023. Research has indicated that by 2025 the number could surpass $10.5 trillion (https://www.evolvesecurity.com).

*Cisco* statistics indicated that the average amount paid for ransom by attack victims was over $300,000 in 2020. *Target*, a general merchandise retailer in the US, paid out $18.5 million in 2017 to settle a large scale data breach that happened in 2013.

**Figure 8 – Cost of cybercrime world wide**




**Source:** www.escudodigital.com

## 7. Conclusions and the way forward

Cybercrime has become rampant throughout the world, especially in those countries where the laws that deal with them are not fool proof. With increased digitalization, globalization, and the advent of block chain technology being used for bitcoin, ethirium, and other such currencies have made it easier for cybercriminals to collect ransom money. It is also easy for them to use these proceeds in unlawful and terrorist activities.

ISSN: 2455-8834

Volume:09, Issue:07 "July 2024"

As the digital world adopts newer and sophisticated technology so do the criminals in hacking datasets form various governments, companies, and individuals. The only way that one can prevent or reduce such crimes is to make the citizens of a country aware of procedures that these criminals tend to follow, and also install sophisticated cybersecurity technology. This is an expensive proposition, but it is definitely cheaper than the value of the information that has been hacked. Besides this governments have to put into place stringent laws for the cybercriminals that are caught. It should be a deterrent for anybody else attempting to get rich in this manner.

**Bibliography**

1. Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258. https://doi.org/10.1016/j.cose.2021.102258

2. Goni, O. (2022). The basic concept of cyber crime. Zenodo. https://doi.org/10.5281/zenodo.6499991

3. Kumar, S. (2020). Cyber crimes in India: Trends and prevention. ResearchGate. https://www.researchgate.net/publication/342142738_CYBER_CRIMES_IN_INDIA_TRENDS_AND_PREVENTION

4. Mullins, M. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(2022), 698–736. https://doi.org/10.1057/s41288-022-00315-5

5. Patil, J. (2020). Cyber laws in India: An overview. ResearchGate. https://www.researchgate.net/publication/349063260_Cyber_Laws_in_India_An_Overview

6. Wadhwa, A. (2016). A review on cyber crime: Major threats and solutions. International Journal of Advanced Research in Computer Science, 8(5), 2217-2221. https://www.researchgate.net/publication/318306240_A_Review_on_Cyber_Crime_Major_Threats_and_Solutions

7. Yayeh, Y. (2022). Cyber security: State of the art, challenges and future directions. ScienceDirect. https://doi.org/10.1016/j.cose.2021.102258