Paradigm Academic Press
Studies in Social Science & Humanities
ISSN 2709-7862
NOV. 2025 VOL.4, NO.6

Cybercrime: A Potential Threat to Global Community

Haradhan Kumar Mohajan[1]

[1] Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh

Correspondence: Haradhan Kumar Mohajan, Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh.

doi: 10.63593/SSSH.2709-7862.2025.11.003

Abstract

Cybercrime is a criminal activity that takes place through the use of computer and internet as instruments for illegal operations. It is a common phenomenon that can take many shapes, and can occur anytime and anyplace through the use of a number of methods, depending on the skill-set and goal of the criminals. It covers a wide variety of criminal activities, such as computer related offences, integrity and availability of computer data, and acts against the confidentiality, content and copyright related offences that create stress on the society in the form of economical disrupt, psychological disorder, threat to national defense, etc. Most of the cybercrimes are done on different parts of the world, and money is the major motivator for many cyber criminals, and still beyond the reach of the law. The cybercrime is a major threat to cyber security and computer data system in the era of globalization due to the rapid spread of information and communication technology (ICT).

Keywords: cybercrime, cyber-security, hacker, virus

1. Introduction

Vinton Gray Cerf is *an American internet pioneer* and is recognized as one of the founders the internet along with American electrical engineer Robert Kahn (Marin, 2005). Cybercrime is a wide range of criminal activities that are carried out using digital devices, hardware devices, and networks that are performed by the use of internet. It is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data (Viswanathan, 2001). Some common cybercrimes are internet fraud, unauthorized access, forgery, cyber-sex, child pornography, cyber pornography, trafficking in child, stealing communication services, online sale of illegal articles, cyber-stalking, phishing, violation of privacy, unsolicited commercial communications, cyber conspiracy, cyber defamation, digital forgery, email bombing, and email spoofing (Vadza, 2013).

Some dangerous cybercrimes are hacking into bank servers, cyber-terrorism, financial crimes, electronic money laundering and tax evasion, terrorism and extortion, economical disrupt, psychological disorder, online gambling, cyber threats, web defacement, telemarketing frauds and illegal telecommunication, and threat to national defense (Tikk, 2011). Among all these cybercrimes, cyber-terrorism has hit mankind with unbelievable severity (Bansal, 2010). These offenses range from criminal activity against data to content and copyright infringement that is raised from the 1980s due to the development of ICT and electronic media (Yar, 2006).

At present people become more computer and internet based (Mohajan, 2025a). As a result, global cybercriminals are engaged in criminal activities without any risk through the use of computer from sitting any far place of the world (Singer & Freidman, 2014). Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. It is done through the network by stealing others important and private data and documents, hacking bank details and accounts, and transferring money to their own (Goni, 2022).

2. Literature Review

A literature review is an overview of previously published works on a particular topic (Phelps, 2018). It is a secondary source and does not report new or original experimental work (Baglione, 2012). *It is the most influential work around any topic* by area, genre, and time. It *demonstrates the ability to do research that* also showcases the expertise on the chosen topic (Galvan, 2015). A good literature review has a proper research question, a proper theoretical framework, and a chosen research methodology (Dellinger, 2005). Osman Goni has described the cybercrime and types of it. He has observed that it is increasing day by day, and it is not only creating human suffering but also puts effects on the economy. The cybercriminals mainly attack the confidential data of organizations, such as hospitals, government offices, police stations, financial institutions, research and development (R&D) organizations, and other telecommunication firms or they target personal information of any person who has valuable assets (Goni, 2022). Sumanjit Das and Tapaswini Nayak have explained a systematic understanding of cybercrimes and their impacts over various areas, such as socio-eco-political, consumer trust, teenager, etc. with the future trends of cybercrimes (Das & Nayak, 2013).

Aurobinda Laha and his coworkers have described that the email bombing is a kind of denial-of-service attack, which is crippling internet. It is a particularly notorious type of the subscription bombing attack, where a victim user's inbox is bombarded with a stream of subscription emails at a particular period (Laha et al., 2022). Priyank Dinesh Gada has shown the arts how credit card hacking works, how smartphones can be hacked, how SIM swapping works, and other techniques with a practical approach. He has warned indicating strategies how to change international mobile equipment identity (IMEI) number and other black hat hacking techniques used by hackers (Gada, 2024). Burak Akdeniz and Aysun Doğan have provided a detailed discussion of cyber bullying with its history, prevalence, effects, risk factors, and protective factors. They have observed that the prevalence of cyber bullying and cyber victimization are quite high among adolescents, and the victims face serious mental health problems (Akdeniz & Doğan, 2024). Udit Agnihotri has mentioned that cyber stalking is the term for when someone is harassed online through various means, such as liking someone's pictures, following their activity, commenting inappropriately, sending unwanted emails and messages that contain obscene content (Agnihotri, 2023).

Amit Kumar Pandey and Rahul R. Kunkulol have shown that cyber pornography has opened up the new environment of save sex. But it has negatively impacted many offline relations, and a new space for sexual predation and exploitation. They have wanted to find out the prevalence, type, and form of risk towards cyber pornography addiction amongst the students (Pandey & Kunkulol, 2017). Naifu Zhang has discussed the definition, type, characteristics, harm of computer virus, anti-virus technology and its application, detection, and removal of computer virus. He has wanted to impart some antivirus knowledge to computer users, and to minimize the possibility of computer users being harmed by computer viruses (Zhang, 2022). Arpit Gajbe and Sir Rahul Chawadha have highlighted the phases of computer virus, history of worst computer attack, type of computer virus with effect on computer, and some examples of virus on their types, working of computer virus, and problem occur due to virus in computers (Gajbe & Chawadha, 2020). Michela Ghelf and his coworkers have wanted to present the current state of knowledge of the risk and protective factors of online gambling. They have investigated greater extent risk factors and variables at the individual level, while protective factors at the relational and contextual level are needed more in-depth study in future research (Ghelf et al., 2024). Muhammad Nadeem and his coauthors have studied a comprehensive review of phishing attacks, their evolution, methodologies, impacts, and countermeasures. Finally, they have provided a valuable reference for academics, cyber security professionals, and policymakers, enabling them to comprehend and address the challenges posed by phishing threats (Nadeem et al., 2023).

3. Research Methodology of the Study

Research is the creation of new knowledge and the use of existing knowledge in a new and creative way so as to generate new concepts, methodologies, and understandings using scientific methods (Cohen & Arieli, 2011). It is a creative and systematic work undertaken to increase the stock of knowledge that involves the collection, organization, and analysis of evidence to increase understanding of a topic, and is characterized by a particular attentiveness to controlling sources of bias and error (Groh, 2018). *Methodology is the plan of action for research. It is a set of methods and principles used to perform a particular activity* (Creswell, 2014). Research methodology is *a systematic framework used to solve the research problem* by using the best and most feasible methods to conduct the research (Kara, 2012). It encompasses the *way in which the intention to carry out the research*. It describes the *techniques and procedures used to identify and analyze information* regarding a specific research topic (Eyler, 2020).

4. Objective of the Study

At present everything runs through the internet, whether it is Google; YouTube; social media platforms, such as Facebook, Instagram, and WhatsApp; and e-commerce websites, such as Amazon, Flipkart, Snapdeal, etc. These make our life simple, but these also expose people to cybercrimes that encompass identity theft, data theft, cyber bullying, cyber stalking, harassment, and other related offences (Agnihotri, 2023; Mohajan, 2025b). Cybercrime is a term used to broadly describe criminal activity in which computers and networks are tool, target, and a place of criminal activity including everything from electronic cracking to denial of service attacks (Das & Nayak, 2013). The main objective of this study is to discuss aspects of cybercrimes. Other minor objectives of the study are as follows (Mohajan, 2017, 2018a,b, 2020):

1) to provide overview of cybercrime, and
2) to discuss the types of cybercrimes.

5. An Overview of Cybercrime

Any crime against the law is committed on computer and internet is known as cybercrime (Kumar, 2001). A wide range of cybercrimes are theft of communication services, electronic money laundering and tax evasion, terrorism and extortion, telemarketing frauds and illegal telecommunication, money laundering, hacking into bank servers, etc. (Krone, 2005). At present internet has provided the opportunities in every field of social media, such as Facebook, Instagram, WhatsApp, Snapchat, and Orkut that give entertainment, business facilities, sports, and educational materials (Heading & Zahidi, 2023). Also, various national and international facilities, such as online shopping, banking, and communication have increased rapidly due to online facilities (Maruf et al., 2010). The criminals destroy the evidence soon after the crime is committed that makes it difficult for the investigating agencies to collect relevant material evidence for prosecuting the offender (Barua & Dayal, 2001).

6. Types of Cybercrimes

There are many types of cybercrimes, such as hacking, email bombing and spamming, cyber terrorism, *cyber bullying*, cyber pornography, virus dissemination, online gambling, web jacking, denial of service attack, cyber stalking, identity theft, credit card fraud, data diddling, phishing, cyber defamation, Salami slicing attack, logic bombs, unauthorized access, sale of illegal articles, computer vandalism, pharming, software piracy, intellectual property crime, etc. (Goni, 2022).

6.1 Hacking

Hacking is the act of finding and exploiting entry points that exist in a computer system or network. It is an unauthorized use of computer and network resources to steal sensitive information or harm the computer system (Goni, 2022; Mohajan, 2025c). It is the most common form of cybercrime that can be used from monetary gain to political interest. It may be in different forms, such as web-spoofing, email bombing, Trojan attacks, phishing, fake websites, spyware, electronic bulletin boards, information brokers, virus attacks, wormhole attack, password cracking, etc. (Fuchs, 2014). The hackers steal files, programs, passwords, and other information from users through the use of internet (Gada, 2024). On the other hand, ethical hacking is permitted by a person or an organization to explore the possibility of vulnerabilities within a system or a network, and the person performing ethical hacking is known as ethical hackers who work with confidentiality, integrity, and availability (Walt, 2017).

Usually the hackers are computer programmers, who have an advanced understanding of computers and commonly misuse their knowledge for devious reasons. There are three types of hackers based on their intent of hacking the system: white hat, black hat, and gray hat hackers (Juneja, 2007). White hat hackers are also known as ethical hackers or IT technicians, and are appointed to check the strength of security, and improve it for the betterment of the company through the making security of the software. They are granted permission by the organization and usually good guys and paid person by the companies with a good thinking (Kumar et al., 2018). They try to find weaknesses, and look for potential security vulnerabilities in the computer system in a legal manner, and can provide solutions in order to re-enforce the computer system and network (Cekerevac et al., 2018). As the growing demands of e-commerce sites, many e-commerce marketing companies like Flipkart, Amazon, and Ebay have demanded more the ethical hackers because of their security concerns (Shimpi & Nagpure, 2015).

The black hat hackers are also known as crackers or malicious hackers within the security industry and modern programmers. They violate the computer system security to gain unauthorized access to the computer system and network in order to destroy, modify, and steal sensitive data (Pal, 2016). They attack banks or other financial organizations with weak security and steal money or credit card information. They break all the security and make network less secure and steal all precious information, compromise the privacy, damage the computer system, and network or block communication (Mallick & Nath, 2024). A grey hat hacker is a mixture of both black hat and white hat hackers, and violate laws but they act without a malicious intent to exploit the security vulnerabilities of the computer system and network. They hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect (Aman & Abhineet, 2017).

6.2 Email Bombing and Spamming

The Email was first sent by American computer scientist Raymond Tomlinson (1941-2016) in 1971, and at present it becomes one of the greatest boons for every modern household, and all sectors of the research and industry. It is used for sending text, documents, and data of tables at home and offices (Laha et al., 2022). Email bombing is a form of net abuse that sends a large volume of emails to a specific recipient for overflowing the mailbox for mail crashing, and most of them are junk or phishing emails but some of them are legitimate regular emails (Schneider et al., 2020). When large amounts of email are directed to a single site, the site may suffer a denial of service through loss of network connectivity, system crashes, and failure of a service due to overloading network connections (Jakobsson & Menczer, 2003). Usually, the email bombing messages are large and constructed from meaningless data in an effort to consume additional system and network resources. Ultimately, the entire mail system will be unusable (Bass et al., 1998). Email phishing is a form of sending messages to determine the recipients of emails to provide information on bank accounts, credit cards, passwords, and other personal details (Şentürk et al., 2017).

Email spamming is a variant of bombing that sends email to hundreds or thousands of users. The purpose of spamming is to attract the email recipients to access some websites and buy more or less legitimate products or services. The spamming can be harmful if the recipients reply to the email, causing all the original addressees to receive the reply (George & Vinod, 2015). It is an intrusive, pervasive, and resource draining distraction that impacts entities at every level. It is almost impossible to prevent, because a user with a valid email address can spam any other valid email address, newsgroup, or bulletin-board service (Xie et al., 2006). The problem of spam has been with us since the 1990s. The email security is the essential tool for business and communication. Unfortunately, there is no way to prevent email bombing and spamming, and it is impossible to predict the origin of the next attack (Chen et al., 2019).

6.3 Cyber Terrorism

At present there is no internationally agreed definition of cyber terrorism. It is the convergence of terrorism and cyberspace. It is an unlawful attack and threat of attacks against computers, networks, and the information stored to intimidate government and its people in furtherance of political, social, and ideological objectives (Nagpal, 2002). It is done by an individual or groups to execute acts of terror. Barry Collin, professor of University of East London, use the word "cyber terrorism" for the first time in the 1980s (Shinde, 2025).

Cyber terrorism is an attack without the use of arms and ammunition but can have the same impact on a nation. It is a new phenomenon that has found expression in the current legal literature on terrorism. It affects adversely the harmony among different religious and racial communities. It is a problem devilling the world and it can take different dimensions (Plotnek & Slay, 2021). The most likely target of cyber terrorists are military installation, power plants, air traffic control, banks, telecommunication networks, fire and rescue system, etc. (Bansal, 2010). Cyber terrorism also poses a serious threat to national security, economic stability, and public safety. It is an unprecedented challenge to global security, national sovereignty, and individual safety (Ottis & Lorents, 2010).

6.4 Cyber Bullying

Cyber bullying is a purposeful and repeated behavior designed to cause physical and emotional distress with a negative effect of online communication between children and teenagers that becomes a great problem in our society, where the victims often experience rumors, and lies spread on online social networks (Lenhart et al., 2010). It is increasing parallel to the rise in internet usage. It involves two people, a bully and a victim. But sometimes it can be carried out by individuals or groups who may be known or unknown persons and consider as the "cancer" of social networks (Akdeniz & Doğan, 2024). It can be discriminative, intentional, repetitive, harmful, and hate crimes, such as sexist bullying, racist and faith targeted bullying, sexual orientation bullying, gender identity bullying, and disabilities bullying (Bayraktar et al., 2015). The digital revolution makes it possible for bullies to harass, threaten, hurt, embarrass, intimidate, humiliate, manipulate, stalk, impersonate, and lie about individual any time from far using an electronic device, such as computer, tablet, and cell phone (Abreu & Kenny, 2018). The bullies may post inappropriate and embarrassing pictures, text messages, etc. of their victims as harassment in email, chat rooms, websites, online games, social networking sites, etc. In some extreme cases, the victims have taken their own lives as a result of cyber bullying (Chisholm, 2014).

6.5 Cyber Stalking

There is no generally accepted definition of cyber stalking as the phenomenon is very recent and relatively lacks detailed knowledge. Cyber stalking is the use of the internet to stalk, harass, control, intimidate, and influence an individual, a group, and an organization through the false accusations, computer monitoring, defamation, slander, libel, threats, identity theft, vandalism, solicitation for sex, doxing, sexual harassment, and blackmail that negatively impact a victim's mental and emotional well-being (Reyns et al., 2011). The stalker may be an online stranger or a known person. S/he pursues the victim through the verbal and written communication, unsolicited single sided romantic involvement, surveillance, harassment and loitering to an extent that the victim suffers from psychological distress and fear (Boon & Sheridan, 2001). Cyber stalking is a new concern in information and communications technology (ICT) for online harassment that is facilitated by low cost, ease of use, and anonymous nature technologies email, texting or instant messages, and social media posts (Chang, 2020).

There are various psychological reasons behind cyber stalking, such as severe narcissism, hatred, rage, retribution, envy, obsession, psychiatric dysfunction, power and control, sadomasochistic fantasies, sexual deviance, internet addiction, and religious fanaticism (Keswani, 2017). For example, a male stalker can manipulate the victim's photos, extorting her to have sex, and if she refuses, threatening to have it leaked online; for one-sided love, the man finds it intolerable that the perpetrator is rejecting him and starts cyber stalking (Agnihotri, 2023). The victim can suffer from anxiety, depression, paranoia, nausea, appetite loss, and insomnia due to constant torture, disruption, blackmail, restlessness, and lack of peace (Spitzberg & Hoobler, 2002). In many countries, cyber stalking is a criminal offense under various state anti-stalking, slander, and harassment laws. It is also a criminal offence motivated by interpersonal hostility and aggressive behaviors stemming from power and control issues (King-Ries, 2011).

6.6 Cyber Pornography

Cyber pornography is an act of using cyberspace to create, display, distribute, impart or publish pornography or obscene materials, child exploitation, and unauthorized distribution through the use of digital platforms, such as websites, social media, emails, and mobile applications (Pandey & Kunkulol, 2017). It refers to all internet usage sexual activities, such as sexual content for recreation, entertainment, exploration, education, trade, and seeking sexual or romantic partners (Agastya et al., 2020). It has a negative impact on lives, beliefs, and relationships of young people; and creates physical, mental, social, and financial problems that lead them to addiction, desensitization unhealthy relationship and sex-violence (Enson, 2017). It plays an accessory role in negative social issues, such as child abuse, violence against women, rape, inequality, relationship and family breakdown, sex-trafficking, youth crime, portraying sex, promiscuity and sexually transmitted diseases (Schneider, 2017). Many factors affect sexual activity, such as gender, knowledge and attitudes, community, and religion (Praveera et al., 2021).

Cyber pornography is a major ethical, legal, and social issue that requires strong laws, public awareness, and preventive measures (Mamun et al., 2019). It has been estimated that about 90% of boys and 60% of girls under the age of 18 have been exposed to pornography (Vinnakota et al., 2021). About 88% porn scenes include acts of physical aggression, 48% contain verbal aggression, and 94% of the target group is women (Bridges et al., 2010). It is found that the majority of boys come under the vulnerable category whereas the girls belong to the low risk group that is affecting their daily life by disconnecting them from the reality (Hald & Mulya, 2013). Child pornography, revenge pornography, and deepfake pornography are serious crimes; and governments, law enforcement, and individuals must work together to prevent these (Chowdhury et al., 2018).

6.7 Virus Dissemination

A computer virus is a type of malicious software programs (malware) that replicates itself by modifying other computer programs and inserting its own code into these programs and negatively affect the functionality of the computer (Piqueira et al., 2008). It is a small program that can be spread from one computer to another and can even affect a computer operation (Parikka, 2007). It can write its own code into the host program, and can infect a computer without permission of a user. If once it gets control, it multiplies itself to form newer generations. When the program of the computer runs, the virus causes infection and damages it (Yeo, 2012). About 50,000 computer viruses provide a variety of effects ranging from the merely unpleasant to the catastrophic (Gole, 2024).

To escape generic scanning, a virus can modify its code and alters its appearance on each infection. Like biological virus, computer virus is contagious, stealthy, infectious, latent, excitable, expressive, and destructive (Zhang, 2022). It results in the loss or damage of hardware, software, data, information, or processing capability of a computer or mobile device. For example, in 1999, the infamous Melissa virus infected thousands of computers and caused damage close to $80 million; while the Code Red worm outbreak in 2001 affected systems running Windows NT and Windows 2000 server and caused damage in excess of $2 billion (Mark, 2006). In May 2000, the ILOVEYOU virus spread worldwide within hours by disguising itself as a romantic email attachment, exploiting vulnerabilities in computers, and infects millions of Windows computers and causing significant disruption and economic damage (Gole, 2024).

In 1949, Hungarian and American mathematician, physicist, computer scientist and engineer John von Neumann (1903-1957) has designed a self-reproducing computer program that is considered first computer virus of the world, and he is considered to be the father of computer virology (von Neumann, 1966). There are many computer viruses, such as boot sector viruses, file viruses, resident virus, non-resident virus, macro virus, polymorphic virus, hoax viruses, Trojan horses, spyware, backdoors, worms, hoax, key loggers, adware, jokers, partition sector viruses, test viruses, logic/time bombs, multipartite viruses (Ludwig, 1996). A virus can be spread in computers if the virus author sends it over the internet or a network, or if it is carried on an infected removable medium, such as a pen drive, CD, flash disk, hard disk, etc. by opening an infected file, running an infected program, through emails, visiting web pages, etc. (Aycock, 2006). It can spread in various ways but the most common ways are fake games, legitimate software updates, pirated software, contaminated systems, and freeware and shareware (Kumar, 2024).

Disasters caused by virus are damaging of programs and software, deleting of files and data on storage devices, corruption of files, slows down of the speed of the computer, formatting of the hard disk, booting failure, taking up of computer memory, and causing of the system crashes (Kephart & White, 1993). Any evidence of infection of a computer by a virus are unusual error messages occurring more frequently, programs taking longer than usual to load, disk accesses seeming excessive for simple tasks, less memory available than usual, access lights turning on for non-referred devices, programs and files disappearing mysteriously, and computer indicating that the storage devices are full (Szor, 2005).

Anti-virus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software, such as viruses and worms. Up-to-date anti-virus software helps users against the latest virus threats (Polk et al., 1995). Some common computer virus scanning software are Norton antivirus software, Backdoor antivirus, McAfee virus scan, AVG antivirus, Avast antivirus, Panda antivirus, Dr. Solomon antivirus toolkit, Web scan antivirus, Kaspersky antivirus, Trend Micro antivirus, Avira antivirus, Logic Bomb antivirus, Rabbit antivirus, Bitdefender antivirus, Smadav antivirus, Symantec antivirus, ESET, HTTP (Hyper Text Transfer Protocol), Thunder byte antivirus, Comodo antivirus, Sophos antivirus, Firewall antivirus, F-secure antivirus, USB disk security, Microsoft Security Essentials, etc. (Filiol, 2007).

6.8 Online Gambling

Gambling is a form of entertainment centered on the wagering of any kind of valuable object or possession on a game or event, whose outcome is predominantly random (Bolen & Boyd, 1968). Online gambling (iGambling) is any kind of gambling, such as virtual poker, casinos, bingo, horse racing betting, private sports betting, betting on billiards or pool, dice game, card games, and sports betting that are conducted on the internet through the electronic devices, such as computers, mobile and smart phones, tablets, and digital television, and its global market is about $40 billion per year (Williams & Wood, 2007). It is global, easily accessible and available 24 hour a day. At present it becomes increasingly popular with children, adolescents, and young adults. Many countries have banned iGambling and increase tax revenues for iGambling in some countries (Griffiths, 2001).

In 1994, small Caribbean nation of Antigua and Barbuda passed the Free Trade & Processing Act, allowing licenses to be granted to organizations applying to open online casinos that effectively allowed US bookmakers to accept bets by phone on horse racing and sports. It has become one of the most popular and lucrative businesses on the internet (Christensen et al., 2015). The money can be transferred with the use of credit card, debit card, electronic check, certified check, money order, wire transfer, etc. (Kumar, 2020). Online gambling has many negative effects on the individual, family, and society. Addicted persons are involved in fraud, theft, extortion, and money laundering in the gambling sites. They face serious side effects, such as social isolation, financial hardships, and scholastic challenges (Benedetti et al., 2025). They can be a cause for smoking, alcohol, and drug addiction, and the individual may even attempt suicide due to depression and emotional breakdown (Vayısoğlu et al., 2019).

6.9 Identity Theft

Identity theft occurs when someone uses an another person's identifying information, such as name, address and telephone number, date of birth, social security number, identifying number, credit card number, driving license number, bank account numbers, bank cards, telephone calling cards, personal identification number (PIN), electronic signatures, fingerprints, passwords, driver's license numbers, etc. without permission of the person to perform various crimes for gaining financial advantages (Hoofnagle, 2007). It is an illicit activity with multiple facets, and is generally included in a larger chain of crimes, such as various frauds, forgery, terrorism, illegal immigration, and money laundering. It is a serious crime against the State or local law that can cause substantial harm to a consumer (Piquero et al., 2021). It is associated with fraud and causes losses for victims of millions of dollars in the world every year. It is a rapidly growing global crime that continues to claim thousands of victims each year with serious consequences (Prosch, 2009). Actually, the identity criminals do no steal identities; instead they use identity as a tool to steal money and doing other crimes. They may run up debts or even commit crimes in victim's name (Dean et al., 2014). They can use identity theft information for purchase goods, property, or services without the consent of victim; create fake financial accounts in the name of victim; obtain cash with bank cards; impersonate victim for financial gain; can rent a luxurious apartment with victim's money; file fraudulent tax returns under victim's name; can file bankruptcy; can give another person's name during an arrest; and can commit other crimes that can damage personal credit and reputation of victim. Millions of people every year are affected both directly and indirectly from identity theft (Albrecht et al., 2011).

Since thieves are able to steal personal information through the internet, fax, regular mail, and telephone, and individuals should not disclose personal information in these media (Collins, 2003). It is wise that anybody should not carry entire identity documents and do not give to swipe the credit and debit cards to anybody. The ATM PIN should be memorized and do not share to anybody. The written documents of personal information should not throw into the garbage and trash bins (Arterberry, 2005). It is imperative that the individuals must create strong passwords with a combination of letters, numbers, punctuation, and special characters that hold a meaning to only the person who created the password (Fordham, 2008).

The term "identity theft" was coined in 1964 that was a time exclusive to physical theft of documents, such as social security cards, credit cards, and driver's licenses. The prevention of it does not lie with only one entity but rather requires the responsibility, cooperation, and actions of three major groups: individuals, businesses, and government (Gilbert & Archer, 2012). The risk of becoming a victim of the identity criminals can be reduced protecting social security number, avoiding phishing, destroying any document contain unprotected personal information, using an identity theft protection service such as LifeLock (Diller-Haas, 2004).

6.10 Phishing

Phishing is a luring type cyber-attack that thieves use to "fish for" unsuspecting internet users' personal identifying information through emails and mirror-websites that the messages appear to come from well-known and trustworthy websites, and pressure has to act quickly, without thinking (Wright, 2016). These email messages often provide links to fraudulent websites where the victims are asked to disclose name, parents name, place of birth, credit card numbers, social security numbers, account numbers, passwords, and other private information (Jansson & von Solms, 2011). Sometimes fake emails come from a reputable and recognize company that offers business proposal. The provided link appears to be the official website of the company, although it is fraudulent (Olivo et al., 2011).

The phishers usually offer their potential victims to share with them a large amount of money that they want to transfer out of their country. Victims are then asked to pay fees, charges to help release or transfer the money. Phishing attackers primarily target individual users and later banking, e-commerce, and social media become prime targets (Ramzan, 2010). The term "phishing" was coined in 1996 by Khan C. Smith, a well-known spammer and hacker. The first phishing is done back to the 1990s by the US black hat hackers and the warez community who were stealing America Online (AOL) accounts by scamming passwords from AOL users (Langberg, 1995). The first known phishing attack against a retail bank was reported in September 2003 (Sangani, 2003).

Spear phishing is an email-spoofing attack that targets a specific organization or an individual, seeking unauthorized access to sensitive information. On the other hand, the whaling phishing is a type of fraud that targets high-profile end users, such as C-level corporate executives, politicians, and celebrities (Lin et al., 2019). An individual can avoid phishing through the ignore of emails which requests to send personal information, contains an offer that is too good to be true, language is urgent, alarming, and threatening, poorly-crafted writing with misspellings, and bad grammar, strange or abrupt business requests, greetings that is ambiguous or very generic, urgency to click on an unfamiliar hyperlinks or attachment (Nadeem et al., 2023).

6.11 Distributed Denial of Service

Denial of service (DoS) attack is one of the major threats and is considered as one of the hardest problem in the internet today. It is an attack in which one or more machines target a victim that attempts to partially or completely prevent the victim from doing useful work, and to stop from viewing portions of the internet (Prakash et al., 2016). It clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. As a result, a legitimate user or organization is deprived of certain services, such as web, email, or network connectivity that the user would normally expect to have. It poses significant threats to network security, disrupting critical services by overwhelming targeted systems with malicious traffic (Jain & Singh, 2012).

There are different types of DoS attacks, such as i) flood attack, that is flooding the target machine with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly as to be made unavailable; ii) logic and software attacks, that is internet packets are sent that should use bugs in the software; and iii) distributed DoS (DDoS) attack, that is either flood attack or logic attack, but it uses many people, different computers, and bots under the attacker's control, and usually attacks target sites, such as banks, credit card payment gateways, etc. (Dzaferovic et al., 2020). The first DDoS attack shutdown the entire internet access on the city for a couple of hours happened in 1997 during a hacker's conference event in Las Vegas by the attacker Khan C. Smith (Lohachab & Karambir, 2018).

The DoS attacks cannot be stopped or prevented, but some precautionary measures are taken into consideration to make the attacker very hard to attack (Nagesh & Sekaran, 2006). The network architecture should be built in a stronger way to secure the resources against various attacks. The host computers must be updated with the latest security patches and techniques (Bhardwaj et al., 2016).

7. Conclusions

Modern world makes our life essay and comfortable. But the varieties of crimes have increased worldwide, and cybercrime is one of them. The cybercrime is a crime that is performed with the help of computer or internet. It is increasing day by day, and normal users are suffering from it, and it is not a national concern anymore rather a matter of global security. The widespread growth of cybercrimes has become a matter of global concern and a challenge for the law enforcement agencies in the new millennium. A comprehensive framework of cyber-security is developing that will provide possible security and privacy threats along with the ways of attacks and countermeasures. Urgent prevention and mitigation of cybercrime is necessary applying combined effort by individuals, organizations, and governments to make cyber security in the society as a priority basis.

References

Abreu, R. L., & Kenny, M. C. (2018). Cyberbullying and LGBTQ Youth: A Systematic Literature Review and Recommendations for Prevention and Intervention. *Journal of Child & Adolescent Trauma*, *11*(1), 81-97.

Agastya, G. N., et al. (2020). Cybersex Addiction: An Overview of the Development and Treatment of a Newly Emerging Disorder. *Medical Journal of Indonesia*, *29*(2), 233-241.

Agnihotri, U. (2023). Cyberstalking: Issues and Challenges. *Amoghvarta*, *3*(2), 171-175.

Akdeniz, B., & Doğan, A. (2024). Cyberbullying: Definition, Prevalence, Effects, Risk and Protective Factors. *Psikiyatride Güncel Yaklaşımlar-Current Approaches in Psychiatry*, *16*(3), 425-438.

Albrecht, C., et al. (2011). How to Protect and Minimize Consumer Risk to Identity Theft. *Journal of Financial Crime*, *18*(4), 405-414.

Aman, G., & Abhineet, A. (2017). Ethical Hacking and Hacking Attacks. *International Journal of Engineering and Computer Science*, *6*(4), 21042-21050.

Arterberry, J. D. (2005). *Identity Theft: Trends, Techniques, and Responses*. The United States Department of Justice: Criminal Division, Washington.

Aycock, J. (2006). *Computer Viruses and Malware*. Publisher: Springer.

Baglione, L. (2012). *Writing a Research Paper in Political Science*. Thousand Oaks, California: CQ Press.

Bansal, M. (2010). Legal Dimensions of Dreaded Cyber Terrorism in India. *Computers & Law*, 20-22.

Barua, Y., & Dayal, D. P. (2001). *Cyber Crimes*. New Delhi: Dominant Publishers & Distributors.

Bass, T., et al. (1998). E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity. *IEEE Network Magazine*, *12*(2), 10-17.

Bayraktar, F., et al. (2015). Cyberbullying: The Discriminant Factors among Cyberbullies, Cybervictims, and Cyberbully-Victims in a Czech Adolescent Sample. *Journal of Interpersonal Violence*, *30*(18), 3192-3216.

Benedetti, E., al. (2025). From policy to practice: assessing the impact of electronic gambling machine regulations on harmful gambling behavior. *Journal of Epidemiology and Community Health*, *79*(9), 726-732.

Bhardwaj, A., et al. (2016). *Three Tier Network Architecture to Mitigate DDOS Attacks on Hybrid Cloud Environments*. ACM Computing surveys.

Bolen, D. W., & Boyd, W. H. (1968). Gambling and the Gambler: A Review and Preliminary Findings. *Archives of General Psychiatry*, *18*(5), 617-630.

Boon, J. C. W., & Sheridan, L. (2001). Stalker Typologies: A Law Enforcement Perspective. *Journal of Threat Assessment*, 1, 75-97.

Bridges, A. J., et al. (2010). Aggression and Sexual Behavior in Best-Selling Pornography Videos: A Content Analysis Update. *Violence against Women*, *16*(10), 1065-1085.

Cekerevac, Z., et al. (2018). Hacking, Protection and the Consequences of Hacking. *Communications*, *20*(2), 83-87.

Chang, W.-C. (2020). Cyberstalking and Law Enforcement. *Procedia Computer Science*, *176*(2020), 1188-1194.

Chen, Z. et al. (2019). Active Learning for Spam Email Classification. In: *Proceedings of the 2nd International Conference on Algorithms, Computing and Artificial Intelligence*, pp. 457-461. Association for Computing

Machinery, New York, USA.

Chisholm, J. F. (2014). Review of the Status of Cyberbullying and Cyberbullying Prevention. *Journal of Information Systems Education*, *25*(1), 77-87.

Chowdhury, R. H., et al. (2018). Does the Addiction in Online Pornography Affect the Behavioral Pattern of Undergrad Private University Students in Bangladesh? *International Journal of Health Sciences*, *12*(3), 67-74.

Christensen, D. R., et al. (2015). Gambling Participation and Problem Gambling Severity in a Stratified Random Survey: Findings from the Second Social and Economic Impact Study of Gambling in Tasmania. *Journal of Gambling Studies*, *31*(4), 1317-1335.

Cohen, N., & Arieli, T. (2011). Field Research in conflict Environments: Methodological Challenges and Snowball Sampling. *Journal of Peace Research*, *48*(4), 423-436.

Collins, J. M. (2003). Business Identity Theft: The Latest Twist. *Journal of Forensic Accounting*, 4, 303-306.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th Ed.). Thousand Oaks: Sage.

Das, S., & Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142-153.

Dean, P. C., et al. (2014). Identity Theft: A situation of Worry. *Journal of Academic and Business Ethics*, *1*(1), 1-14.

Dellinger, A. B. (2005). Validity and the Review of Literature. *Research in the Schools*, *12*(2), 41-54.

Diller-Haas, A. (2004). Identity Theft: It Can Happen to You. *CPA Journal*, *74*(4), 42-44.

Dzaferovic, E., et al. (2020). DoS and DDoS vulnerability of IoT: A review. *Journal of Sustainable Engineering and Innovation*, *1*(1), 43-48.

Enson, S. (2017). Evaluating the Impact of Pornography on the Lives of Children and Young People. *British Journal of School Nursing*, *12*(7), 325-330.

Eyler, A. A. (2020). *Research Methods for Public Health*. New York: Springer Publishing Company.

Filiol, E., et al. (2007). Evaluation Methodology and Theoretical Model for Antiviral Behavioral Detection Strategies. *Journal in Computer Virology*, *3*(1), 27-37.

Fordham, D. R. (2008). How Strong are Your Passwords? *Strategic Finance*, *89*(11), 42-47.

Fuchs, C. (2014). Anonymous: Hacktivism and Contemporary Politics. In: Idem (Ed.), *Social Media, Politics and the State*, pp. 88-106. New York: Routledge.

Gada, P. D. (2024). The Art of Hacking. *Journal of Emerging Trends and Novel Research*, *2*(12), a73-a84.

Gajbe, A., & Chawadha, S. R. (2020). Computer Virus: Their Problems & Major attacks in Real Life. *Journal of Emerging Technologies and Innovative Research*, *7*(8), 652-659.

Galvan, J. L. (2015). *Writing Literature Reviews: A Guide for Students of the Social and Behavioral Sciences* (6th Ed.). Pyrczak Publishing.

George, P., & Vinod, P. (2015). Machine learning approach for filtering spam emails. In: *Proceedings of the 8th International Conference on Security of Information and Networks*, pp. 271-274. Association for Computing Machinery, New York, USA.

Ghelf, M., et al. (2024). Online Gambling: A Systematic Review of Risk and Protective Factors in the Adult Population. *Journal of Gambling Studies*, *40*(2), 673-699.

Gilbert, J., & Archer, N. (2012). Consumer Identity Theft Prevention and Identity Fraud Detection Behaviors. *Journal of Financial Crime*, *19*(1), 20-36.

Gole, D. (2024). Computer Viruses. *National Journal of Hindi & Sanskrit Research*, *1*(56), 64-67.

Goni, O. (2022). Cyber Crime and Its Classification. *International Journal of Electronics Engineering and Applications*, *10*(1), 1-17.

Griffiths, M. (2001). Internet Gambling: Preliminary Results of the First U.K. Prevalence Study. *Journal of Gambling Issues*, *5*(5), 1-9.

Groh, A. (2018). *Research Methods in Indigenous Contexts*. New York: Springer.

Hald, G. M., & Mulya, T. W. (2013). Pornography Consumption and Non-Marital Sexual Behaviour in a Sample of Young Indonesian University Students. *Culture, Health & Sexuality*, *15*(8), 981-996.

Heading, S., & Zahidi, S. (2023). *The Global Risks Report 2023* (18th Ed.). World Economic Forum.

Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law & Technology*, *21*(1), 97-122.

Jain, A., & Singh, A. K. (2012). Distributed Denial of Service (DDoS) Attacks: Classification and Implications. *Journal of Information and Operations Management*, *3*(1), 136-140.

Jakobsson, M., & Menczer, F. (2003). Untraceable Email Cluster Bombs: On Agent-Based Distributed Denial of Service. CoRR, cs.CY/0305042.

Jansson, K., & von Solms, R. (2011). Phishing for Phishing Awareness. *Behaviour & Information Technology*, *32*(6), 584-593.

Juneja, G. K. (2007). Ethical Hacking: A Technique to Enhance Information Security. *International Journal of Innovation Studies*, *3297*(12), 7575-7580.

Kara, H. (2012). *Research and Evaluation for Busy Practitioners: A Time-Saving Guide*. Bristol: The Policy Press.

Kephart, J. O., & White, S. R. (1993). Measuring and Modeling Computer Virus Prevalence. Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy.

Keswani, M. H. (2017). Cyber Stalking: A Critical Study. *Bharati Law Review*, 2017, 131-148.

King-Ries, A. (2011). Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future? *Texas Journal of Women and the Law*, *20*(2), 131-164.

Krone, T. (2005). *High Tech Crime Brief*. Australian Institute of Criminology. Canberra, Australia.

Kumar, D., et al. (2018). Towards the Impact of Hacking on Cyber Security. *IIOABJ Journal*, *9*(2), 61-77.

Kumar, K. (2001). *Cyber Laws Intellectual Property & E-Commerce*. Dominant Publishers & Distributors.

Kumar, S. (2020). Online Gambling. Indian Legal Solution. https://indianlegalsolution.com/online-gambling/

Kumar, V. (2024). Computer-Virus: Types and Its Preventation. *Journal of American Science*, *20*(5), 9-12.

Laha, A., et al. (2022). SubStop: An Analysis on Subscription Email Bombing Attack and Machine Learning Based Mitigation. *High-Confidence Computing*, *2*(2022), 100086.

Langberg, M. (1995). *AOL Acts to Thwart Hackers*. San Jose Mercury News.

Lenhart, A., et al. (2010). *Social Media & Mobile Internet Use among Teens and Young Adults*. Pew Internet & American Life Project, Washington, DC.

Lin, T., et al. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction*, *26*(5), 32.

Lohachab, A., & Karambir, B. (2018). Critical Analysis of DDoS: An Emerging Threat over IoT Networks. *Journal of Communication and Information Networks*, *3*(3), 57-78.

Ludwig, M. A. (1996). *The Little Black Book of Computer Viruses: Volume 1, The Basic Technologies*. American Eagle Publications.

Mallick, A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69.

Mamun, M. A., et al. (2019). Attitudes and Risk Factors of Pornography Consumption among Bangladeshi University Students: An Exploratory Study. *International Journal of Mental Health and Addiction*, *17*(2), 323-335.

Marin, G. A. (2005). Network Security Basics. *Security & Privacy*, *3*(6), 68-72.

Mark, S. (2006). *Information Security Principles and Practice*. John Wiley & Sons, Inc., Publication.

Maruf, A. M., et al. (2010). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. *The Northern University Journal of Law*, *1*(2010), 112-124.

Mohajan, H. K. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University Economic Series*, *17*(3), 58-82.

Mohajan, H. K. (2018a). Aspects of Mathematical Economics, Social Choice and Game Theory. PhD Dissertation. University of Chittagong, Chittagong, Bangladesh.

Mohajan, H. K. (2018b). Qualitative Research Methodology in Social Sciences and Theoretical Economics. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

Mohajan, H. K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People*, *9*(4), 50-79.

Mohajan, H. K. (2025a). Machine Learning: A Brief Review for the Beginners. Unpublished Manuscript.

Mohajan, H. K. (2025b). Artificial Intelligence: Prospects and Challenges in Future Progression. Unpublished Manuscript.

Mohajan, H. K. (2025c). Deep Learning: A Brief Study on Its Architectures and Applications. Unpublished Manuscript.

Nadeem, M., et al. (2023). Phishing Attack, Its Detections and Prevention Techniques. *International Journal of Wireless Security and Networks*, *1*(2), 13-25.

Nagesh, H. R, & Sekaran, K. C. (2007). Proactive Solutions for Mitigating Denial-of-Service Attacks. *International Journal of Computer Science and Network Security*, *7*(7), 167-175.

Nagpal, R. (2002). Defining Cyber Terrorism. *The ICFAI Journal of Cyber Law*, *1*(1), 77.

Olivo, C. K., et al. (2011). Obtaining the Threat Model for E-mail Phishing. *Applied Soft Computing*, *13*(12), 4841-4848.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, pp. 267-270. Reading: Academic Publishing Limited.

Pal, S. (2016). Overview of Hacking. *IOSR Journal of Computer Engineering*, *8*(4), 90-92.

Pandey, A. K., & Kunkulol, R. R. (2017). Cyber Pornography Addiction amongst Medical Students of Western Rural Maharashtra. *International Journal of Clinical and Biomedical Research*, *3*(2), 10-14.

Parikka, J. (2007). Digital Contagions: A Media Archaeology of Computer Viruses. New York: Peter Lang.

Phelps, R. P. (2018). *To Save the Research Literature, Get Rid of the Literature Review*. LSE Impact Blog, London School of Economics.

Piqueira, J. R. C., et al. (2008). Dynamic Models for Computer Viruses. *Computers & Security*, *27*(7-8), 355-359.

Piquero, N. L., et al. (2021). Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders. *Victims & Offenders*, *16*(3), 444-463.

Plotnek, J. J., & Slay, J. (2021). Cyber Terrorism: A Homogenized Taxonomy and Definition. *Computers & Security*, *102*(2), 102145.

Polk, W. T., et al. (1995). Antivirus Tools and Techniques for Computer Systems. William Andrew: Elsevier.

Prakash, A., et al. (2016). Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture. *Procedia Computer Science*, *87*(2016), 275-280.

Praveera, K. H., et al. (2021). Cyber-Pornography Addiction among Medical Students of Telangana. *Indian Journal of Public Health*, 1*2*(1), 303-309.

Prosch, M. (2009). Preventing Identity Theft throughout the Data Life Cycle. *Journal of Accountancy*, *207*(1), 58-62.

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. In Stamp, Mark; Stavroulakis, Peter (Eds.). *Handbook of Information and Communication Security*. Springer.

Reyns, B. W., et al. (2011). Being Pursued Online: Applying Cyberlifestyle: Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169.

Sangani, K. (2003). The Battle against Identity Theft. *The Banker*, *70*(9), 53-54.

Schneider, J. P. (2017). Effect of Cybersex Addiction in the Family. *International Journal of Biomedical and Clinical Research*, *7*(1-2), 31-58.

Schneider, M., et al. (2020). Diving into Email Bomb Attack. *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 286-293, IEEE.

Şentürk, Ş., et al. (2017). Email Phishing Detection and Prevention by Using Data Mining Techniques. In: *International Conference on Computer Science and Engineering*, pp. 707-712, IEEE.

Shimpi, P. P., & Nagpure, S. (2015). Penetration Testing: An Ethical Way of Hacking. *Global Journal for Research Analysis*, *9*(6), 611-614.

Shinde, N. V. (2025). Cyber Terrorism: The Emerging Threat in the Digital Age. *International Journal for*

Multidisciplinary Research, *7*(2), 1-6.

Singer, P. W., & Freidman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the Technologies of Interpersonal Terrorism. *New Media & Society*, *1*(4), 71-92.

Szor, P. (2005). *The Art of Computer Virus Research and Defense*. Boston: Addison-Wesley.

Tikk, E. (2011). Ten Rules for Cyber Security. *Survival: Global Politics and Strategy*, *53*(3), 119-132.

Vadza, K. C. (2013). Cyber Crime & Its Categories. *Indian Journal of Applied Research*, *3*(5), 130-133.

Vayısoğlu, K. S., et al. (2019). The Frequency of Gambling Among University Students and Its Relationships to Their Sensation. *Addicta: The Turkish Journal on Addictions*, *6*(1), 69-90.

Vinnakota, D., et al. (2021). Pornography and Sexual Violence against Women in India: A Scoping Review. *Journal of Psychosexual Health*, *3*(3), 216-221.

Viswanathan, S. T. (2001). *Bharat's the Indian Cyber Laws with Cyber Glossary* (2nd Ed.). New Delhi: Bharat Law House.

von Neumann, J. (1966). *Theory of Self-Reproducing Automata: Essays on Cellular Automata*. University of Illinois Press.

Walt, C. D. (2017). The Impact of Nation-State Hacking on Commercial Cyber-Security. *Computer Fraud and Security*, *2017*(4), 5-10.

Williams, R. J., & Wood, R. T. (2007). Internet Gambling: A Comprehensive Review and Synthesis of the Literature (Report). Guelph, Ontario, Canada: Ontario Problem Gambling Research Centre.

Wright, A. (2016). The Big Phish: Cyberattacks against US Healthcare Systems. *Journal of General Internal Medicine*, *31*(10), 1115-1118.

Xie, M., et al. (2006). An Effective Defense against Email Spam Laundering. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 179-190, Association for Computing Machinery, New York, USA.

Yar, M. (2006). *Cybercrime and Society*. London: Sage Publications.

Yeo, S.-S. (2012). *Computer Science and Its Applications: CSA 2012, Jeju, Korea*. Springer.

Zhang, N. (2022). Computer Virus and Anti-Virus Technology. 3rd International Conference on Language, Art and Cultural Exchange. *Advances in Social Science, Education and Humanities Research*, pp. 91-103, Atlantis Press.

Copyrights