Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol.11 No.1, 2022, pp.36-45
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajeat-2022.11.1.3309

An Overview on Cyber Crime and Cyber Security

Bhumika Tuli[1], Santosh Kumar[2] and Neha Gautam[3]
[1]Department of Computer Science and Engineering, [2]Department of Mechanical Engineering,
[1&2]Chandigarh Group of Colleges, Mohali, Punjab, India
[3]St. Ezra International School, Mohali, Punjab, India
E-mail: santoshdgc@gmail.com

(Received 15 March 2022; Revised 12 April 2022; Accepted 10 May 2022; Available online 20 May 2022)

***Abstract* - Loss of information through online services is called a "footprint of cybercrime". So, the topic that we will discuss is Cyber Crime and Cyber Security. It is an important part of the information technology field. We all know that cybercrime is increasing day by day, and the government also takes measures to stop this, but it's not dying from its root. In this research paper, we will discuss about the different phases of cybercrime in today's time and the negative effects tolerated by people due to cybercrime. There are so many financial loses hanging over from heavy engagement in cybercrimes that have been discussed below. This paper also consists of topics related to cyber security, which provides safety to users. Overall, this article gives an intensive overview regarding cybercrime, the work of criminals and the cyber security and because of it how to prevent the cybercrime and make it secure, as new technology is there that comes up with new ideas to protect human life.**

***Keywords:* Cybercrimes, Cyber Security, Online Scams**

I. INTRODUCTION

Cybercrime footprints are spreading like a coronavirus discovered in China. It attacks human life, mainly that of children and mature humans. Cybercrime is one of the fastest growing areas [1]. Similarly, a large number of activities carried out by criminals are done with the help of ICT tools. There are so many developed gadgets like mobile phones, laptops, etc. that are used by humans that work like robots and help to reduce the pressure that is on the human's mind, but it does not mean that they have only advantages, as they have many effects regarding insecurity and cybercrime. Major human actions include call fittingness, financial transactions using mechanics finance, and email transmissions [2]. Similarly, there is an increase in size among children and women in India through chat rooms today. It has increased their growth by 50% over the previous year [3]. Some examples related to cybercrimes that rise up in India through social media are that in the year 2017, it was 328,whereas in 2016 it was 155[4]. This may affect India in a large variety of ways. The internet is used all over the world, and it has become a visual part of people's lives. And it creates a breed of social hacking and makes a person's life damaged.

Activities that involve computers, network devices, or a network are called "cybercrime." A large number of criminal activities are carried out with the assistance of ICT tools and their applications [5]. The main areas that are covered or attacked by criminals are failures of security, loss of availability, loss of discretion, and destructive physical activity [6]. This phenomenon is only known to hackers and cyber criminals. Hackers, cyber-criminals, and terrorists are also becoming more sophisticated.

Through methods that are not commonly shared within the general security community and are carried out under the cover of security [7]. Today's generation wants modish gadgets such as cloud computing, mobile computing, e-commerce, and net banking to get a high degree of privacy. People want positive restrictions to make their data safe and their lives safer too. Data security measures always lead to privacy and security. Digital forms have maintained all the data in today's world. The fight against cybercrimes needs an enlargement of security [8].

Every individual accepts responsibility for reducing these types of crimes. Governments also place many restrictions and make laws to prevent the types of cases that are done in a wide range of countries, especially in India [9]. There are some other scams from which people save their information or data. There are some open-minded questions regarding how to stay safe online: (a) what to do if you have fallen for a scam; (b) if you download malicious software; (c) if you send money to a person (fraud); (d) if your credit or debit card information is stolen; (e) if your entire identification is stolen [10]. Hence, the objectives of the current study are

1. To enquire about the current status of the illegal threat in BRICS.
2. To verify the ways that makes BRICS nations lucrative targets, mainly for cyber criminals.
3. An access to the impact of cybercrimes attacks on these economics.
4. Some advice for it in order to find a reasonable solution to this problem.

Cybercrime is an illegal activity committed by commissions and thefts using various gadgets such as computer. There are different types of cybercrimes which have a high rating at the present time, and these crimes have been done with the help of network intrusions, dissemination of computer viruses and computer-based changes of existing crimes like identity theft, stalking, bullying and terrorism which is not a minor problem for human life [12].

II. TYPES OF CYBER CRIMES

There are distinct types of cybercrime as depicted in Figure 1 and discussed below.

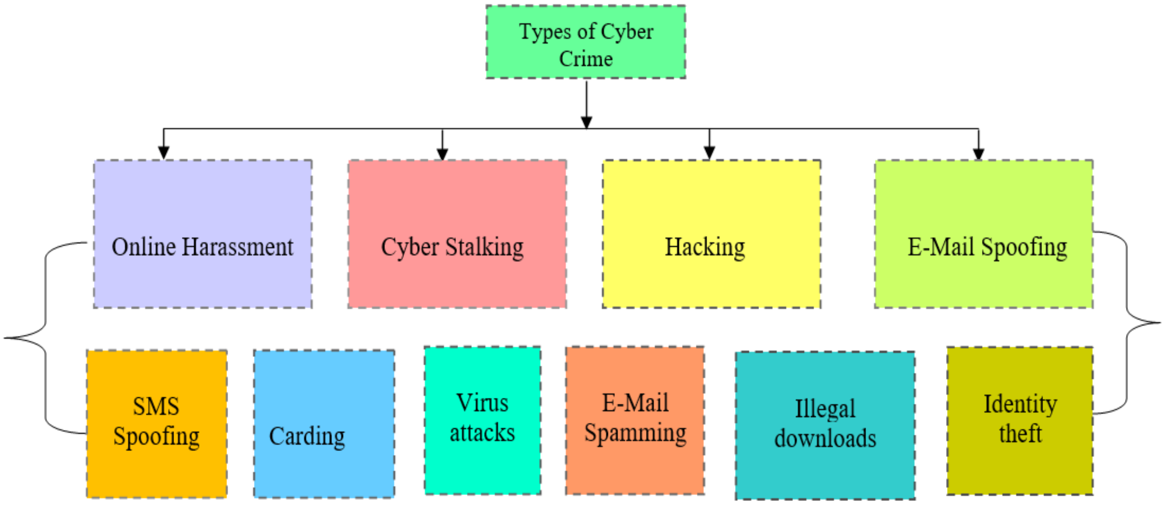

Fig. 1 Types of cybercrimes [13]

1. Online Trolling: It includes sharing badgering symbols, marks, types, characters etc., through electronic mails [14]. These all are done on social media. In this case, a troll is a person who posts inflammatory content on an online forum. It also means attacking on any person directly by doing online trolling.

2. Hacking: Hacking is the collection and deletion of personal or private data. It is a social networking site on which there is a stealing of personal information through hacking, which is also a weakness of the computer system [15]. It includes the sharing of fake electronic mail to social website users, including fake operator directions. It is basically used for sending phishing emails to shut down business communication. These emails number in the hundreds and are sent to hundreds of people in less than a minute [16].

3. Entails Blocking Unwanted Messages: These SMS basically lead to the theft of bank information by making calls in a fraudulent manner. There are some calls that are for gaining profits by getting another person’s data, such as bank account numbers, passwords, and OTP.

4. Carding: In this, criminals use fees on ATM cards and debit cards to withdraw money. Firstly, hackers hack personal data by making illegal calls and then making threats using users’ details by making fake cards.

5. Virus Attacks: In this type of attack, criminals create harmful viruses and then release them into computers to damage and delete personal information. In this, hackers do anything on other people’s accounts. They can add any type of video, photos, etc.

6. Email Spamming: sending thousands of emails to different users, and all these emails are under fake conditions, which may be used to steal users’ data [17].

7. Illegal Downloads: Downloading of the latest games and movies is also called cybercrime. For example, there are some apps that are made by hackers for hacking data or specifically for gaining profit, such as Blue Whale Game and PUBG. In these games, players have to purchase some cards with money, so in this way, hackers gain profit [18].

8. Identity Theft: This refers to a crime where criminals use victims to conduct online transactions. There are some other victims also, like scams that have been used by hackers or criminals [19].

A. Cyber Threat Landscape on BRICS

Basically, BRICS stands for Brazil, Russia, India, china and South Africa and BRICS has been able to get their leading positions in the world economy by acting as unofficial consumer marketers. These are the five nations that face many changes in their time and have different structures in their lives. There are a large number of people that are on social media, which means they use internet in a static position, especially among the citizens of BRICS [20] (Figure 2). Cyber criminals are the new developing threats that are spreading all around us. There are a few internal sources of threats like employees of agencies, customers and end users of companies [22].

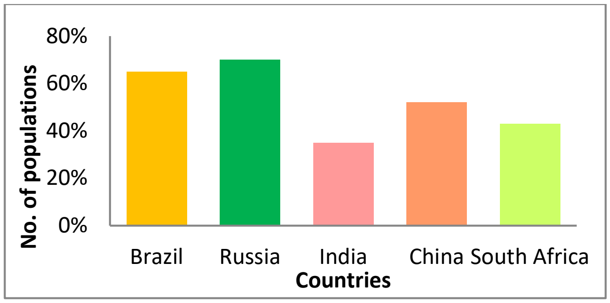

Fig. 2 Country wise consumption

B. Impact of Cyber Crime on Different Stages

1. Footprints of Cyber Crime Over Teenagers: Nowadays, most teenagers are mingling with cyber work, which may create many problems in today's generation. It is common to all [23]. Children below eighteen come under this action as they do not have any knowledge. Mostly females come under this negative situation because hackers think that women do not have any power so that they catch them [24]. However, when it comes to males, there are few cases of hacking because hackers believe they have the power to do something new, such as hacking a case concerning cybercrime [25].

2. Footprints of Criminal Offence Over User Deportment: The data revolution, integrated with the raging of the internet, exposes a number of open societies to the danger of cybercrime. Cooperation should realize the different threats. These markers are considered a coin as internet privacy has been upgraded to check the privacy of consumers' security and free shopping. Cybercrime is the sole cause of both prosperity and poverty, and it is growing by the day as we all see that it affects the entire world [27]. India has the largest chunk of global poor because of cybercrime [28] (Figure 3).

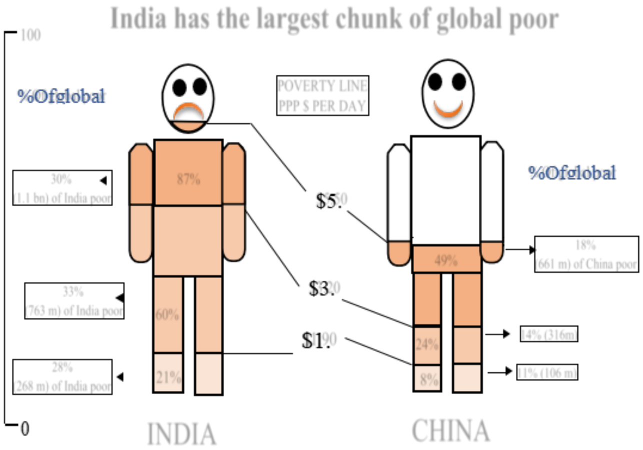

Fig. 3 Largest chunk of global poor [28]

III. CAUSES OF PROSPERITY AND POVERTY

As cybercrime increases day by day and the users in the world are in a high range and they do not live without it (Figure 4). There are so many cases when user do anything on internet, some pop ups come between the using time which is mostly related to crimes such as gaining of money by playing illegal games [29].

There are some more examples that in case of banks, fraud calls are also there in which hackers tell the users id, passwords and many more and if user give them all then he/she may lose all his/her money. These types of crimes make a powerful money man to lower money man which creates so many problems for that person.

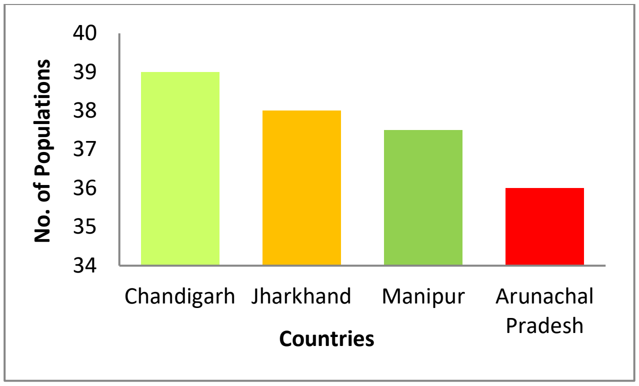

Fig. 4 Case of poverty due to cybercrimes [30]

IV. COMPUTER SECURITY

Any ancient crimes that are conducted through web are cybercrimes and saving it from others by any tool is called cyber security (Figure 5). The work of protecting the data or any of the information from hackers is also called cyber security. There are so many technological solutions to safeguard the trapping of any of the computer network or the personal information that leads to cyber security [31].

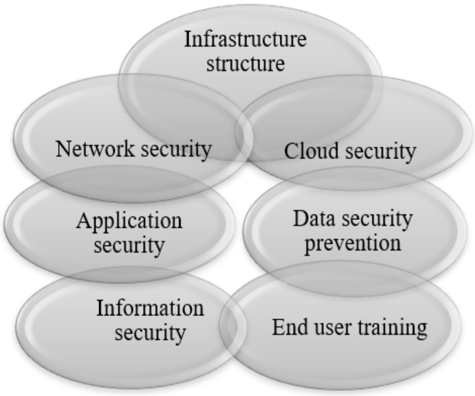

Fig. 5 Computer security [32]

There are so many strategies through which we can secure our data easily. The government should take actions or restrictions regarding all these crimes.

1. It should be a way to increase the punishment for cyber-crime.
2. There should be an increase in the action of death by taking action.
3. Always accept cyber terrorism.
4. There should be enough manpower to improve all the management regarding the increment of cyber-crime that is done only by hackers [33].

Privacy and security of information are measures, that any cooperation takes care of it. In this, all data is stored digitally in the form of cyber data. It is the location where all users save their collections on each piece of hardware. Cyber security plays a fatal role in today's generation. In many countries, there is no understanding of control because of cybercrime [34]. Online arrangements are currently secured through private activities, laws, enforcement and other forms of international cooperation. Cyber security is being played by non-governmental authorities.

V. TECHNICAL MEASURES

Technical measure may be of two types (a) International measure and (b) National measure.

Domestic governments always get together with each other to protect someone's personal data by exchanging information, investigating attacks, stopping harmful conduct, providing evidence, or even arranging a request for the rendition of individuals.

An international agreement always depends upon activities like cyber security [35]. Most national governments enact their own legislation to punish cyber criminals. They suggest some national laws for the protection of sharing and attacks on governments like NSA to collaborate in the creation of cyber-attacks. There is a necessity related to cyber security which helps people's data and secures their information from cyber criminals to get more safety in life. These are the only one measuring techniques that have no effect on anyone [36].

A. Social Media Resources

There are so many applications that have been used, especially for the security of human data, to defend all pertain related to outsider crimes, viruses, or any of the attacks that have been conducted by cyber criminals. At the time of the development of social networking sites, first note that there is a case of crime in this situation, so while developing all these sites, they also make a point of cyber security and how to save our data from threats [37].

B. Communication Security, Which Includes Some of the COMSEC Disciplines

COMSEC stands for "Communication Security." It is used for protecting or securing data from telephonic communication. It also helps in writing any information and in transferring it to another device through any of the stages. It decodes data on the site of the sender and makes it unreadable until that data is inscribed on the receiver side [38].

1. Emission Security: This security is used to provide relief from the capture of material.

2. Physical Security: It enhanced by the dissemination of all-prevention cryptographic information, documents, and data.

3. Transmission Security: it is that security that has been working when any of the data has to be transferred from one device to another device to secure all the personal information, preventing the stealing of data by malicious people [39].

4. Information Security is A Term that Leads to the Term Information Technology: It is used for securing data as well as taking part in the protection of software and hardware items. This security has done its work in the process of business, how to manage data or how to create documents for meetings. There is a word that comes under information security that is named "integrity": it is basically for the modification of data [40]. The various cyber stalking categories are shown.

C. Communication Security

Basically, COMSEC stands for communication security. It is used for protecting or securing data from telephonic communication. It also helps in writing any information and in transferring it to another device via any of the stages. It encrypts data on the sender's side and renders it unreadable until it is rewritten on the receiver's side [41].

1. Emission Security: This security is used to provide relief from the capturing of material.

2. Physical Security: It is relieved by sharing its entire cryptographic information, documents, and information prevention.

3. Transmission Security: it is that security that has been put to work when any of the data has to be transferred from one device to another device to secure all the personal information against stealing of data by malicious people [42].

4. Information Security: Information security is a name that leads to information technology. It is used in securing data as well as taking part in protection of software and hardware things. This security has done its job in the business process of managing data or creating documents for meetings. There is a word that comes under information security that is named "integrity": it is basically for the modification of data [77]. The various cyber stalking categories are shown in Table I.

TABLE I CATEGORY OF CYBER STALKING EMAIL [43]

1	Stalking transfer of viruses through emails and messages is a cyber threat, especially to get their personal ID's zip-code.
2	Internet stalking sharing of photos and personal data in front of others on social networking sites.
3	Computer stalking is basically connecting one device to another device in order to hack it by performing operations on it.

D. Network Security

This security is used for securing the parts of networking from one device to another or a connection over networking. Network security has so many layers, and each layer works for different purposes in security, and all these purposes lead to the networking of cyber threats only [44]. All of the components that work in networking security collaborate to make their security materials less timeconsuming and more powerful in terms of information security [45]. Operational security includes some of the security-based tools such as

1. Operational Security: OPSEC is a special name that is given to operational security, as it is the main security tool for securing anything. Opportunity security is basically used for controlling or managing the whole system regarding the making of plans for any of the security.

2. Identify Critical Information: First we have to check what type of data is there that is harmful to an organization if the data is obtained by a customer, employee, or from any other adversary [46]. The second step for controlling is to determine which code is there that is given by the user for their private information, and this is a big target for the user that he/she should find with a bit of big data.

3. Analyze Vulnerabilities: In the next stage, union representatives check the impotence of the safe-conduct to secure the personal data, and then they find a sphere or a destination where a lack of security department training leaves subject matter open to attack.

4. Asses' Risks: The third step in operational security is that many companies make their attacks for the purpose of destroying the opinion of data, so an organizer must take a decision on how to break all these attacks that have been made by other departments of cyber threat.

5. Apply Appropriate Countermeasures: This is the final step of control by making a plan by mixing all the stages that have been given above and making a huge box of attacking other people who are under all these cyber threats [47]. They also develop or upgrade new technologies with the help of government policies.

E. Cyber Security Risk Management

All risks that create problems for human resources in their lives that cause panic conditions are based on three factors.

1. Threats: People who have already done their work in hacking They do their work of theft, like stealing another's data, spoiling the whole computer system, stealing personal data by using government policies, doing hacking for other countries, and people who are involved in hacking for non-state purposes. So, to decrease these outputs, developing capabilities have been upgraded for security.

2. Vulnerabilities: These are systems that are so complex that they can be hacked. It is almost the same as malicious software [48]. If any of the attackers do any type of fraud in the database, they use vulnerable hacking as a fraud [49].

3. Viruses: This is the element that causes a major issue for a user. It is linked to your device without your permission or knowledge [50]. Viruses are basically defects or defects that destroy our computers' files. There are so many fake mails, messages that have been sent by the sender (fraud) for hacking or to distract others' information through online mode. Viruses operate on gadgets on social networking sites as well. Example: Melissa, Sesser, and Code: red [51]. These are the examples of viruses which may extend day by day. Table II indicates the different virus's categories.

TABLE II VIRUSES CATEGORIES [52]

1	*Habitant Virus:* This virus is done only on target system. This virus is activated only when operating system is going to start.
2	*Non- Resident Virus:* This is the virus that directly effects on networking location and with local systems. This virus does not take rest in system for a longer duration of time.
3	*Bang Sector Virus:* This virus is being loaded in memory where there is a boot is invented from the destroyed life.

4. Worms: Worms are different from viruses in that there is no need for a host to control them. Once the effects begin in any computer, they automatically run. Warms is also known as malicious software. It does not take any free memory from internal sites; it works as an outsider [53]. Example: Ineffective transportation, Bagle, Blaster.

TABLE III WORM CATEGORIES [54]

1	*Telecommunicate Worms:* These are that worms which is being share through emails, messages etc.
2	*Computer Network Worms:* It is sharing over the internet through making link by illegal methods.
3	*Web Worms:* It shares that network which is not good for users as it has no privacy.

5. Trojan Horses: It is the major problem for users, as this is that hacking which is done by ending fake emails or messages to any person and steal their personal information by asking questions like they have a jackpot for you and for this you have to tell me your personal ID zip code and like this they hack all the information by the users [55]. It also harms the computer system or others gadgets also by sending files which consist of bag full with viruses. Table IV indicates that what the different types of Trojan are.

TABLE IV TYPES OF TROJAN [56]

1	*Power of Attorney Trojan:* It is the type of trojan which is used to make a scientific structure through proxy server, which helps in playing different operations.
2	*Watchword Stealer Trojan:* This is used for stealing any type of password from the computer system.
3	*IM Trojan:* It is used to steal the personal information , any kind of data from any social networking sites such as from face-book, Instagram, Skype etc.
4	*Pipette Trojan:* It is used to make other malicious software or malware software. This Trojan is used in the initialization of the attack.
5	*Game Thief Trojan:* This Trojan is used for getting any other person's data by playing games in online mode.
6	*Trojan-Banker:* This Trojan is used in stealing bank account information like as passwords of credit card or debit card.

This is the hacking that has been done by fraudsters. In this, hackers crack others' ID passwords with the help of any software and get all the personal information of others. That is called illegal work.

VI. FINDINGS OF THE STUDY

The study of awareness of cybercrimes is the biggest weapon required to subordinate the data [57]. There are a total of 200 outcomes taken as a sample of this education, and this sample is done only at the age range of 18-27 yrs. If we take an example, these respondents were from different colleges, such as Rajagiri, Amrita Vishwa Vidyapeetham, SCMS, Maharaja's College, SNGIST, St. Xavier's College for Women, etc., [58]. Figure 10 indicates how many males there are that are under cybercrime and how many females there are that come under cybercrime [59]. There are so many findings related to cybercrime.

A. Findings on Cybercrime and Awareness

Cybercrime spreads all over the world by 25.1%, through which 51.7% know what cybercrime is and 21.7% do not have any knowledge about cybercrime, while only 1.7 [60]. 95% have no idea how cybercrime works. 8% of respondents understand what fraud is. 71.8% of total respondents understand cyber interaction. 53.7% are unaware of identity theft. 59.6% are aware of credit card and debit card fraud. 9% of respondents say that it is necessary to be secure while using the internet and 22.1% agree with it, while 5.8% do not give their response to it because they all disagree [61]. 8% of the total respondents were overcharged due to cybercrime. 2.4% of the respondents have transactions that are under fraud investigation. Money has been lost by 3.8% of the respondents. 76% had not lost their money due to cybercrime [62].

B. Findings on the Precautions of College Students

64% use antivirus software for their own use, especially for their mobile phones, desktops, laptops, computer etc., The remaining respondents do not use antivirus for their mobile phones or digital gadgets that are now developing day by day. 59% of the respondents use passwords on mobile phones, computers, laptops, or when opening new sites to save their data from cybercrimes and hackers, so that they are not able to steal their data. 46.8% use pin numbers in their gadgets for security, 46.8% use fingerprints, and only 6.8% use face lock [63]. 9% of the respondents changed their passwords when they saw the alert. Only 3.6% of the respondents changed their passwords once a week in a month. Every 2-week password has been changed by 3.6% of the respondents. 6% check the verification of websites they use before entering them, and 31.5% check their websites on a regular basis.12.1% of the respondents check their websites when they have a look at it [64].

C. Cyber Safety Tips for Cyber Security

This is the type of hacking in which there no email is sent by the bank to notify you that your account has been compromised, but it asks you to give your personal data like a password or pin, which it already has [65]. So do not give it to them.

1. Smart phones take the place of pocket-sized desktops: This is the kind of hacking that directly attacks your laptop and desktop. To secure this, create a strong password.
2. Keep your personal information to yourself: Do not write any personal information on the entire page of any social networking site, such as on Instagram, Facebook, or Twitter. Also, do not put your birth date. Because of this, your bank account has been hacked [66].
3. Know the pitfalls of public Wi-Fi: We should always avoid taking others' wireless internet connections.
4. Beware of public computers: Do not access your personal information or data on another computer because they have keystrokes that record your password, account number, or other personal information [67].
5. Use credit card rather than debit card: When you purchase anything anywhere, if you do not have cash, then you use a card, so in this case, you should always use a debit card, because it has a lower chance of fraud [68].
6. Purchase only from reputable websites: It is so easy to create an online market store and sell stuff by creating a store. Those sites come under fraud for making fake stores and collecting people's credit card information, so do not trust any of the online shopping or other sites [69].
7. Check your accounts and your credit reports regularly for errors. You have to check your credit data every day to ensure that fraudulent accounts have not been created in your name and that all these mechanisms have been created on annual com.
8. Avoid suspicious e-mails: Do not click on any of the links, whether they are shared by your friend or through your relative. First, know everything about that site, and then go with it. The most common cyber threat to detect theft is email viruses [70].

D. An Approach to Reduce Cyber Crime

As cybercrime starts in developing countries and it also creates so many issues in their lives, after realizing all these effects that are caused by cybercrime, some of the institutions to combat cybercrime are being built in developing countries [72]. There is an example of destroying this negative effect: In Romania, there is a town named Ramnicu Valence, where fraud cases are settled in large amounts. In 2005, there were two officers who were there to deal with more than 200 cases by using a computer, having aged nine years and having no internet connection [73]. To connect any of the devices with another, they use the same cafes that were used by cyber criminals to connect the networks. In this way, they use the same theme that had been used by the hackers to resolve the problem that had been on the heads of the consumers and sit on it as a panic condition comes under them. In Bangladesh, people come under hacking. They use subscriber identity modules in their cell phones, and this idea has been spread all over Bangladesh; not even a single town has left [75].Countries from different parts of the world made the security products only to handle cyber networks. In order to protect themselves from hackers, North America created 58 percent of the privacy items for their own country in 2002 [76].Sixty percent of Kenyan banks have a secure system, according to the findings. There are so many mechanisms that are being used by China for the improvement of things, but the concept that has been adopted by China is "hollow diffusion" of online and e-commerce upgrading among firms in growing countries [77].

VII. CONCLUSION

As we recover from all the topics related to cybercrime and how to reduce it, that means cyber security. So, we study that the big hand behind cybercrime is developing gadgets. As they help us in various conditions, they also create a hamper blast for users. The hacker's identity ranged from 12 years old to 67 years old. To give the path of decrement to cybercrime, there is a term called "cyber security." There are eight paths which help us prepare to fight against cybercrime: Enable the automatic update on your computers, there is no need to share your personal information with any other person, install firewalls, Report the id's of those who are doing any type of crime, these are some of the saved lists that saved a human life.

VIII. RECOMMENDATIONS

Some of the suggestions have been given by the department of information and technology of Nepal and all these suggestions are only for cyber security through which people saves their personal information and data, so that they can hide their data with a powerful link as a powerful tool [78]. All these suggestions are given below.

1. Make more complex passwords by adding special characters, numbers, alphabetic letters or by some of the gaps such as small or capital letters through which we can secure our data and always use a different user ID [79].
2. Always ignore an unknown ID. If any message has come from any of the unknown ID'S ignore it or put it into the bin. Do not reply to that email. It may be a message in a fraud case [80].
3. Do not respond to that email especially which is asking about your personal information, passwords, your pin-code, OPT's, ATM numbers etc.
4. Check your account with any of the bank ID'S daily on the basis of securing your data [81].
5. Always exercise caution when communicating via online dating [82].
6. We do not have to share our personal information as a biography on any of the accounts.
7. Always accept those friend requests; those are known only to us [83].
8. Some people create fake IDs in order to contact others and also to hack other users' data.
9. Do not share any personal information on social media [84]. If you want to post it, then put it as a private.
10. Avoid malicious downloads if there is no need.
11. Always remember protection by Phishers [85].
12. Do not install any of the apps that are doing malicious work.
13. Need human value education [86-88].

REFERENCES

[1] S. Gii and R. L. Shrestha, "Reform of civil service of Nepal with e-government practice," *Journal of Personnel Training Academy,* Vol. 6, No. 1, pp. 22-36, 2018.

[2] R. J. Harkneet and J. Stever, "The cyber security triad: Government, private sector partner, and the engaged cybersecurity citizen," *Journal of Homeland Security and Emergency Management,* Vol. 6, No. 1, pp. 79, 2009.

[3] A. M. Dario Sgobbi and Marco Paggio, "Intrusion in a Mission Critical Network: A Tutorial on Intrusion Detection Systems and Intrusion Prevention Systems," *Modelling Cyber Security,* 2009.

[4] E. C. Chang and J. Xu, "Remote integrity check with dishonest storage serve," *Proceedings of the 13th European Symposium on Research in Computer Security,* pp. 223-237, 2008. [Online]. Available: http://www.vox.com/2014/5/19/5731696/chinesehackers-cyberespionage-theft-cyber.

[5] Grispos, George, Sorren Hanvey and Bashar Nuseibeh, "Use of Organizational Topologies for Forensic Investigations," pp. 2-5, 2017. [Online]. Available: http://www.theregister.co.uk/2013/03/27/stuxnet_cyverwar_r.

[6] S. Parto, "Economic activity and institutions: taking stock", *Journal of Economic Issues,* Vol. 39, No. 1, 2005. DOI: 10.2202/1547-7355.1649.

[7] D. Kumar and N. Panchanatham, "A case study on Cyber Security in E-Governance," *International Research Journal of Engineering and Technology (IRJET),* Vol. 2, No. 8, pp. 272-265, 2015. [Online]. Available: http://www.europarl.europa.eu/meetdocs/20142019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[8] L. Serena, "A Fuzzy Approach to Security Codes: Cryptography between Technological Evolution and Human Perception," *Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.) IOS Press,* 2009. [Online]. Available: http://www.aseanstats.org.

[9] A. T. Kearney, *Cyber security in ASEAN- AN Urgent Call to Action,* 2018. [Online]. Available: https://www.cisco.com/c/dam/m/ensg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf.

[10] D. K. Mulligan and F. B. Schnelder, "Doctrine for cybersecurity," *Daedalus,* Vol. 140, No. 4, pp. 70-92, 2011. [Online]. Available: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdfcountry-1=TH.

[11] P. Sitbon, "A Cyber Security Approach for Smart Meters at ERDF," *Modeling Cyber Security: Approaches, Methodology, Strategies, U. Gori (Ed.),* 2009. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/The cost-of-Cyber-Crime-Summary-Final.pdf.

[12] H. J. Mohammed, E. AL-dahneem, A. Hamadi, "A comparative analysis for adopting an innovative pedagogical approach of flipped teaching for active classroom learning," *J. Glob. Bus. Soc. Entrep.,* Vol. 3, No. 5, pp. 86-94, 2016. https://www.mha.gov.sg/Newsroom/press-releases/Pages/Computer-Misuse-and-Cybersecurity-(Amendment)-Bill-.aspx.

[13] Bagyavati, "Social Engineering in Lech J. Janczewski and Andrew M. Colarik Cyber warfare and cyber terrorism," Vol. 1, No. 1, pp. 9-15, 2009. [Online]. Available: http://capec.mitre.org/data/definitions/117.html.

[14] Ravi Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society,” *International Journal of Scientific & Engineering Research,* Vol. 3, pp. 67-75, 2012. [Online]. Available: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html.

[15] D. Ahlstrom and G. D. Bruton, “Learning from successful local private firms in China: establishing legitimacy,” *Academy of Management Executive,* Vol. 15, No. 4, pp. 72-8, 2001. [Online]. Available: http://business.rediff.com/slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.html.

[16] D. Denning, “An Intrusion-Detection Model,” *IEEE Transactions on Software Engineering,* Vol. SE-13, No. 2, pp. 222-232, 1987. [Online]. Available: http://www.cyberlawsindia.net.

[17] A. Sreehari, K. J. Abinanth, B. Sujith and P. S. Unnikuttan, “A Study of Awareness of Cyber Crime Among College Students with Special Reference to Kochi,” Vol. 119, No. 16, pp. 1353-1360, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Demographics_of_India.

[18] N. Tan, “Social networking: Danger - Warning for Teens,” *International Journal of Internet of Things,* Vol. 1, No. 1, pp. 9-15, 2008. [Online]. Available: http://cis-india.org/internet-governance/cyber-crime-privacy.

[19] J. E. Oxley and B. Yeung, “E-commerce readiness: institutional environment and international competitiveness,” *Journal of International Business Studies,* Vol. 32, No. 4, pp. 705-723, 2001. [Online]. Available: http://worldwidejournals.com/paripex/file.php?val=March_2016_1458622776_05.pdf.

[20] S. Bistarelli and F. Fioravanti and P. Peretti, “Using CP-nets as a guide for countermeasure selection,” *Proceedings of the 2007 ACM Symposium on Applied Computing,* pp. 300-304, 2007. [Online]. Available: http://www.cs.kent.ac.uk

[21] D. K. Mulligan and F. B. Schnelder, “Doctrine for cybersecurity,” *Daedalus,* Vol. 140, No. 4, pp. 70-92, 2011. [Online]. Available: http://www.gov.uk.

[22] N. Kshetri and N. Dholakia, “Professional and trade associations in a nascent and formative sector of a developing economy: A Case Study of the NASSCOM effect on the Indian offshoring industry,” Vol. 15, No. 2, pp. 225-239, 2009.

[23] A. M. Dario Sgobbi and Marco Paggio, “Intrusion in a Mission Critical Network: A Tutorial on Intrusion Detection Systems and Intrusion Prevention Systems,” *Modelling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.),* 2009.

[24] H. J. Mohammed, M. M. Kasim, E. A. AL-Dahneem and A. K. Hamadi, “An analytical survey on implementing best practices for introducing e-learning programs to students,” *J. Educ. Soc. Sci.,* Vol. 5, No. 2, pp. 191-196, 2018. http://taylorandfrancis.com.

[25] R. J. Harkneet and J. Stever, “The cybersecurit triad: Government, private sector partner, and the engaged cybersecurity citizen,” *Journal of Homeland Security and Emergency Management,* Vol. 6, No. 1, pp. 79, 2009. [Online]. Available: http://www.cs.kent.ac.uk.

[26] I. D. Fianyi, “Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics,” *International Journal of Computer Science Issues,* Vol. No. 5, No. 12, 2015. [Online]. Available: http://business.kaspersky.com/threats- in-q2

[27] N. Kshetri, “Positive externality, increasing returns and the rise in cybercrimes,” *Communications of the ACM,* Vol. 52, No. 12, pp. 141-144, 2009. [Online]. Available: freedom-of-expression-amnesty-intl/.

[28] I. D. Fianyi, “Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics,” *International Journal of Computer Science Issues,* Vol. No. 5, No. 12, 2015. [Online]. Available: http://business.kaspersky.com/threats- in-q2

[29] S. Back and J. LaPrade, “Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 25-47, 2020, [Online]. Available: http://www.justice.gov.

[30] D. Kumar and N. Panchanatham, “A case study on Cyber Security in E-Governance,” *International Research Journal of Engineering and Technology (IRJET),* Vol. 2, No. 8, pp. 272-265, 2015. [Online]. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html.

[31] BSA, *BSA Global Cloud Computing Scorecard, A Blueprint for Economic Opportunity,* 2013. [Online]. Available: http://arxiv.org/abs/1106.4692v1.

[32] M. Sharma, H. Jindal, S. Kumar and R. Kumar, “Overview of data security, classification and control measure: A study”, *I-managers Journal on Information Technology,* Vol. 11, No. 1, pp. 17-34, 2022. [Online]. Available: https://imanagerpublications.com/article/18557/13.

[33] R. J. Harkneet and J. Stever, “The cybersecurity triad: Government, private sector partner, and the engaged cybersecurity citizen,” *Journal of Homeland Security and Emergency Management,* Vol. 6, No. 1, 2009. [Online]. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html.

[34] M. D. T. P. Nasution, A. P. U. Siahaan, Y. Rossanty and S. Aryza, “The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop,” *International Journal of Civil Engineering and Technology (IJCIET),* Vol. 9, No. 6, pp. 1583-1592, 2018. [Online]. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html.

[35] M. D. T. P. Nasution, A. P. U. Siahaan, Y. Rossanty and S. Aryza, “The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop,” *International Journal of Civil Engineering and Technology (IJCIET),* Vol. 9, No. 6, pp. 1583-1592, 2018. [Online]. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html.

[36] L. Serena, “A Fuzzy Approach to Security Codes: Cryptography between Technological Evolution and Human Perception,” *Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.),* 2009. [Online]. Available: http://www.indiancybersecurity.com.

[37] D. Kumar and N. Panchanatham (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology (IRJET), Vol. 2, No. 8, pp. 272-265, http://www.indiancybersecurity.com.

[38] A. M. Dario Sgobbi and Marco Paggio, “Intrusion in a Mission Critical Network: A Tutorial on Intrusion Detection Systems and Intrusion Prevention Systems,” *Modelling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.),* 2009. [Online]. Available: http://www.indiancybersecurity.com.

[39] European Union, “The Convention on Cyber-Crime, a unique instrument for international co-operation,” *IJARCET,* Vol. 6, 2001. [Online]. Available: http://www.indiancybersecurity.com.

[40] D. Kumar and N. Panchanatham, “A case study on Cyber Security in E-Governance,” *International Research Journal of Engineering and Technology (IRJET),* Vol. 2, No. 8, pp. 272-265, 2015. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[41] ITU, “ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia, Meeting Report: ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia”, pp. 25-28, 2008. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[42] S. Back and J. LaPrade, “Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 25-47, 2020. [Online]. Available: https://cltc.berkeley.edu/scenario-back-matter.

[43] W. Fadzilah, W. Yusoff, and A. B. Sade, “Electronic banking fraud ; The need to enhance security and customer trust in online banking,” *International Journal in Advances in Information Sciences and Service Sciences,* Vol. 3, 2008. [Online]. Available: https://www.bitdegree.org/tutorials/what-is-cyber-security.

[44] M. T. Whitty, “The Online Romance Scam: A Serious Cybercrime,” *Cyberpsychology, Behavior, and Social Networking,* Vol. 15, No. 3, 2011. [Online]. Available: https://www.getgds.com/resources/blog/cybersecurity/6-cybersecurity-threats-to-watch-out-for-in-2021.

[45] Riccardo Satta, Javier Galbally, and Laurent Beslay “Children Gender Recognition Under Unconstrained Conditions Based on Contextual Information,” *International Conference on Pattern Recognition,* pp. 357-362, 2014. [Online]. Available: www.zdnet.com/article/cybercrime-costs-338bn-to-globaleconomy-more-lucrative-than-drugstrade/.

[46] ITU, “ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia, Meeting Report: ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia”, pp. 25-28, [Online]. Available: www.gov.uk/government/ publications/the-cost-of-cybercrimejoint-government-and-industry-report.

[47] C. Subramanian, “Cyber Security,” *International Journal of Recent Scientific Research,* Vol. 3, No. 3, pp. 197-200, 2012. [Online]. Available: http://veriscommunity.net.

[48] D. K. Mulligan and F. B. Schnelder, “Doctrine for cybersecurity,” *Daedalus,* Vol. 140, No. 4, pp. 70-92, 2011. [Online]. Available: http://gigaom.com/2011/11/16/thereal-costs-of-cybercrime-infographic.

[49] R. J. Harkneet and J. Stever, “The cybersecurity triad: Government, private sector partner, and the engaged cybersecurity citizen,” *Journal of Homeland Security and Emergency Management,* Vol. 6, No. 1, 2009. [Online]. Available: www.virusbtn.com/conference/vb2004/abstracts/sgarfink.xml.

[50] Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Larry Korba, Ronggong Song and George Yee, “An analysis of online gaming crime characteristics”, *Internet Research,* Vol. 15, No. 3, pp. 246-261, 2005. [Online]. Available: www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisathreat-landscape/enisa-threat-landscape.

[51] Grispos, George, Sorren Hanvey, and Bashar Nuseibeh, “Use of Organisational Topologies for Forensic Investigations”, *Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics,* pp. 2-5, 2017. [Online]. Available: http://www.nccgroup.com/media/169256/origin_of_ hacks q32012.pdf.

[52] R. Tillman, K. Calavita and H. Pontell, “Criminalizing white-collar misconduct: determinants of prosecution in savings and loan fraud cases,” *Crime Law and Social Change,* Vol. 26, No. 1, pp. 53-76, 1996. [Online]. Available: http://www.nccgroup.com/media/169256/origin_of_hacks_q3_2012.pdf.

[53] S. Alshathry, “Cyber-attack on saudi aramco,” *Int. J. Manag.,* Vol. 11, No. 5, 2016. [Online]. Available: http://www.nccgroup.com/media/169256/origin_of_hacks_q3_2012.pdf.

[54] S. Zeadally, E. Adi, Z. Baig and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” *IEEE,* pp. 23817-23837, 2020. [Online]. Available: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf.

[55] A. D. Smith and W. T. Rupp, “Application service providers (ASP): moving downstream to enhance competitive advantage,” *Information Management & Computer Security,* Vol. 10, No. 2, pp. 64-72, 2002. [Online]. Available: http://discover.ukdatas_ervice.ac.uk/catalogue/?sn=5543&type=Data%20catalogue.

[56] indolink.com, India battles against cybercrime, 2012. [Online]. Available: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf.

[57] R. G. Sarita Sharma, “Comparative Study and Analysis of Unique Identification Number and Social Security Number,” *International Journal of Scientific Research in Computer Science and Engineering,* Vol. 5, No. 1, pp. 27-30, 2017. [Online]. Available: http://www.sophos.com/en-us/security-news-trends/securitytrends/fake-antivirus.aspx.

[58] D. Kumar and N. Panchanatham, “A case study on Cyber Security in E-Governance,” *International Research Journal of Engineering and Technology (IRJET),* Vol. 2, No. 8, pp. 272-265, 2015. [Online]. Available: https://www.birminghammail.co.uk/news/midlandsnews/school-meals-coronavirus-text-scam-17975311.

[59] M. Stohl, “Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime, law and social change,” Vol. 46, No. 4-5, pp. 223-238, 2006. [Online]. Available: https://www.birminghammail.co.uk/news/midlandsnews/school-meals-coronavirus-text-scam-17975311.

[60] R. M. Fishman, K. Josephberg, J. Linn, J. Pollack and J. Victoriano, “Threat of international cyberterrorism on the rise,” *Intellectual Property & Technology Law Journal,* Vol. 14, No. 10, pp. 23-23, 2002. [Online]. Available: https://www.birminghammail.co.uk/news/midlandsnews/school-meals-coronavirus-text-scam-17975311.

[61] Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Larry Korba, Ronggong Song and George Yee, “An analysis of online gaming crime characteristics”, *Internet Research,* Vol. 15, No. 3, pp. 246-261, 2005. [Online]. Available: https://www.birminghammail.co.uk/news/midlandsnews/school-meals-coronavirus-text-scam-17975311.

[62] Grispos, George, Sorren Hanvey and Bashar Nuseibeh, “Use of Organisational Topologies for Forensic Investigations”, Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics, pp. 2-5, 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/newcoronavirus-screenlocker-malware-is-extremelyannoying.

[63] S. Back and J. LaPrade, “Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 25-47, 2020. [Online]. Available: https://blog.checkpoint.com/2020/05/12/coronaviruscyber-attacks-update-beware-of-the-phish.

[64] BSA, *BSA Global Cloud Computing Scorecard, a Blueprint for Economic Opportunity,* 2013. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/04/22/there-are-now-more-than-40000-high-risk-covid-19–threats-on-the-web.

[65] E. C. Chang and J. Xu, “Remote integrity check with dishonest storage serve, “r. Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, (ESORICS’08), ACM Press, Heidelberg, pp. 223-237, 2008. [Online]. Available: https://www.fda.gov/consumers/health-fraudscams/fraudulent-coronavirus-disease-2019-covid-19-products.

[66] Raymond Dacey and S. Kenneth Gallant, “Crime control and harassment of the innocent,” *Journal of Criminal Justice, Elsevier,* Vol. 25, No. 4, pp. 325-334, 1997. [Online]. Available: https://ec.europa.eu/anti-fraud/media-corner/news/20-03-2020/olaf-launches-enquiry-fake-covid-19-relatedproductsen.

[67] George Grispos, Sorren Hanvey and Bashar Nuseibeh, “Use of Organisational Topologies for Forensic Investigations”, *Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics,* pp. 2-5, 2017. [Online]. Available: https://www.gov.uk/government/news/uk-medicinesand-medical-devices-regulator-investigating-14-casesof-fake-or-unlicensed-covid-19-medical-products.

[68] S. Mierzwa, S. RamaRao, J. A. Yun and B. G. Jeong, “Proposal for the development and addition of a cybersecurity assessment section into technology involving global public health,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 48-61, 2020. [Online]. Available: https://cltc.berkeley.edu/scenario-back-matter.

[69] Thievery, Embezzlement and Fraud, “New York: Thomas Y. Crowell Company,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 62-66, [Online]. Available: https://www.bitdegree.org/tutorials/what-is-cyber-security.

[70] S. Back and J. LaPrade, “Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 25-47, 2020. [Online]. Available: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.html.

[71] B. Nodeland, “The effects of self-control on the cybercrime victim-offender overlap,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 4-24, 2020. [Online]. Available: http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx.

[72] BSA, *BSA Global Cloud Computing Scorecard, a Blueprint for Economic Opportunity,* 2013. [Online]. Available: https://hmaconsulting.com/projects/kuwait-general-department-of-criminal-investigation.

[73] H. J. Mohammed, E. AL-dahneem and A. Hamadi, “A comparative analysis for adopting an innovative pedagogical approach of flipped teaching for active classroom learning,” *J. Glob. Bus. Soc. Entrep.,* Vol. 3, No. 5, pp. 86-94, 2016. [Online]. Available: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Global.

[74] Brenner, “Social networking dangers exposed,” 2009. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[75] Bagyavati, “Social Engineering in Lech J. Janczewski and Andrew M. Colarik Cyber warefare and cyber terrorism, Vol. 1, No. 1, pp. 9-15, 2009. [Online]. Available: http://www.symantec.com.

[76] A. Kumar, “Orkut used in credit card scam to buy airline tickets,” *The Deccan Chronicle,* Vol. 1, No. 1, pp. 9-15, 2008. [Online]. Available: http://www.symantec.com.

[77] T. Rid, “Think again: cyberwar,” *Foreign Policy,* Vol. 192, pp. 1-11, 2012. [Online]. Available: http://www.indiancybersecurity.com.

[78] N. Kshetri, “Positive externality, increasing returns and the rise in cybercrimes,” *Communications of the ACM,* Vol. 52, No. 12, pp. 141-144, 2009. [Online]. Available: http://www.frankrubino.com.

[79] S. Bistarelli, F. Fioravanti and P. Peretti, “Using CP-nets as a guide for countermeasure selection,” *Proceedings of the 2007 ACM Symposium on Applied Computing,* pp. 300-304, 2007. [Online]. Available: http://arxiv.org/abs/1106.4692v1.

[80] N. Jyoti, “Cyber Security: Protection of Human Rights,” Vol. 3, No. 2, pp. 888-895, 2017. [Online]. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html.

[81] B. Nussbaum, Book review of Whiteside, Thomas, “Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. New York: Thomas Y. Crowell Company,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 62-66, 2020. [Online]. Available: http://arxiv.org/abs/1106.4692v1 .

[82] W. Lifei, H. Zhu, C. Zhenfu and W. Jia, Sec Cloud, “Bridging secure storage and computation in cloud,” *Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, IEEE Xplore Press,* Genova, pp. 52-56, June 21-25, 2010. [Online]. Available: http://www.justice.gov.

[83] OECD, Cybersecurity policy making at a turning point: Analysing new generation of national cybersecurity strategies for the internet economy, 2012. [Online]. Available: http://business.kaspersky.com/threats- in-q2-2013.

[84] H. Choi, H. Lee, H. Lee and H. Kim, “Botnet Detection by Monitoring Group Activities in DNS Traffic,” *in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007),* pp. 715-720, 2007. [Online]. Available: https://en.wikipedia.org/wiki/Demographics_of_India.

[85] S. Back and J. LaPrade, “Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions,” *International Journal of Cybersecurity Intelligence and Cybercrime,* Vol. 3, No. 2, pp. 25-47, 2020. [Online]. Available: http://business.rediff.com/slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.html.

[86] S. Rani, H. Beenu Jindal, N. Gautam, and S. Kumar, “Importance of Universal Human Values for Human life: A Study”, *Asian Journal of Science and Applied Technology,* Vol. 11, No. 1, pp. 36-48, 2022. DOI: https://doi.org/10.51983/ajsat-2022.11.1.3204.

[87] H. Jindal, Y. Garg, S. Kumar, N. Gautam, and R. Kumar, “Social media in political campaigning: A Study”, *I-manager’s Journal on Humanities & Social Sciences,* Vol. 16, No. 1, pp. 49-60, 2021. [Online]. Available: https://imanagerpublications.com/article/18266/.

[88] S. Aman Kumar, S. Sharma, and R. Kumar, “Importance of Universal Human Values in Education System: A Critical Review”, *I Manager’s Journal of Humanities & Social Science,* Vol. 1, No. 2, pp. 45-55, 2020.