Hindawi
Journal of Computer Networks and Communications
Volume 2018, Article ID 1798659, 11 pages
https://doi.org/10.1155/2018/1798659

Review Article

Cybercrimes: A Proposed Taxonomy and Challenges

Harmandeep Singh Brar[1] **and Gulshan Kumar**[2]

[1]*Department of Computer Applications, Maharaja Ranjit Singh Punjab Technical University, Bathinda, India*
[2]*Department of Computer Applications, Shaheed Bhagat Singh State Technical Campus, Ferozepur, India*

Correspondence should be addressed to Harmandeep Singh Brar; harmanbrar22@gmail.com

Received 15 December 2017; Accepted 27 March 2018; Published 12 April 2018

Academic Editor: Youyun Xu

Cybersecurity is one of the most important concepts of cyberworld which provides protection to the cyberspace from various types of cybercrimes. This paper provides an updated survey of cybersecurity. We conduct the survey of security of recent prominent researches and categorize the recent incidents in context to various fundamental principles of cybersecurity. We have proposed a new taxonomy of cybercrime which can cover all types of cyberattacks. We have analyzed various cyberattacks as per the updated cybercrime taxonomy to identify the challenges in the field of cybersecurity and highlight various research directions as future work in this field.

1. Introduction

In this modern age, the world is becoming more familiar and close to each other by means of Internet and new networking technologies. The networking infrastructure is the base for information sharing among individuals, private sectors, and military and government sectors. Approximately 50% of the world population has an Internet connection up to January 2017. There is a rise of 10% in the Internet users from January 2016 to January 2017 [1]. According to [2], in 2016, there are 6.4 billion connected devices and this will reach 20.8 billion by 2020. The present world technologies of hardware and software give new wings to the process of connecting various devices (mobiles and smartwatches) with Internet. Anybody can get, see, and share information on the Internet from any place in this world. There is a huge growth of Internet-connected devices from the past to the present which give rise to the area of the cyberspace. The growth of Internet users in the world and world population is shown in Figure 1.

During the last five years, we observed that an increasing number of data, devices, and clouds were forming a perfect security storm of threats. Some of the threat predictions became true which are leading significance of much bigger storm expected in the near future. The dynamicity in the work place, highly mobile work strength, and frequently changing expectations of workers have changed the concept of network boundary. The flood of personal network devices has created an exponential growth of personal data on the Internet. According to [3], the number of devices will continue to grow in both volume and variety, and they predict that this number will reach 200 billion by 2020 and continue to grow in the future. So, the cyberspace is expanding everyday. This expansion has given rise to the various opportunities for cybercriminals to do malicious acts on the Internet and also given rise to the difficulty level for security professionals to put a security umbrella on the entire cyberspace. It is clear from the above discussion that the cyberspace has a huge volume of data and information that is available on the Internet and its resources must be protected from cybercriminals [3].

Every individual is doing some work to fulfill his/her objective. The objective may be to gain money, respect, revenge, or any other. Cyberattackers also have objectives for which they do cyberattacks/cybercrimes. Here, we will discuss the most common objectives of cyberattackers.

(1) Entertainment. Some cybercriminals perform their activities of cyberattack to test their hacking abilities. They feel proud and joy in their successful attempts.

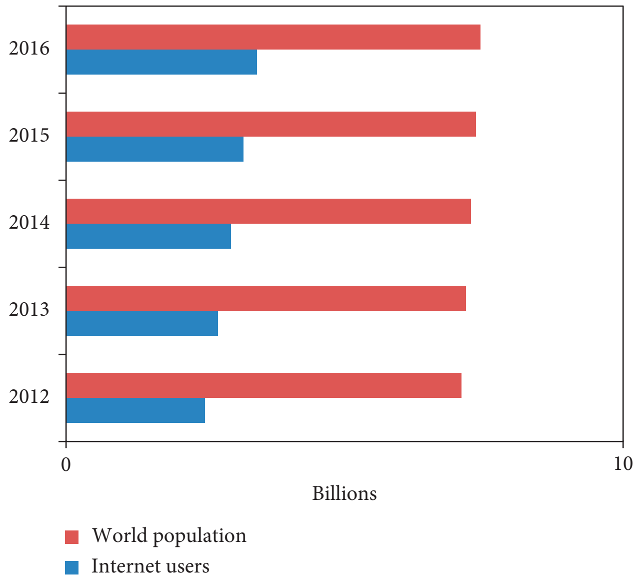

Figure 1: Internet users in the world.

They are willing to get fame in the world of cybercriminals. They feel joy and proud when they make an attack which was not performed by any other attacker or other attackers failed to perform that attack.

(2) Hacktivists. These cyberattackers are motivated by political, religious, and social ends. Their motive is to preach their political and religious mottos and to discourage the people of other sets. They want to extend their religion or politics to make them popular among the masses. The current trend of 2016 and 2017 shows that hacktivists are exposing the individuals having secret affairs through social websites. The latest example is Ashley Madison dating whose users list was exposed by attackers in public domain.

(3) Financial gain. Most of the cyberattackers perform the cyberattacks for financial gain. They desire to become rich. The target of cyberattackers may be the banking system, big companies, organizations, rich individuals, or wealthy countries. Some of these cyberattackers are either hired by some country, organization, company, or individual.

(4) Spying. These types of cybercriminals attack the networks to steal the confidential information of specific country, organization, or individual. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid in return.

(5) Revenge. These types of cybercriminals include the expelled, irritated, and humiliated employees. They knew the policies, secrets, and weak points of their company, organization, or country. They perform their activities of cyberattacks under the emotion of hate to take their revenge in the form of financial loss, tarnishing their social image, reputation, and so on.

In this paper, we conduct the survey of cybersecurity of recent prominent researches in context to various security principles, namely, confidentiality, integrity, and availability in the field. We categorize the recent incidents of cybersecurity on the basis of these fundamental principles and propose a new taxonomy of various cybercrimes. We have analyzed various security attacks as per the updated taxonomy to identify the challenges in the field and highlight various research directions as future work in the field.

To facilitate the discussion of cybersecurity, Section 2 introduces the cybersecurity and the fundamental principles of cybersecurity. In Section 3, the various types of environments affected by cybercrimes in the past few years have been discussed. Section 4 gives the introduction of various types of cybercrimes. The introduction about various types of cyberattacks is discussed according to the fundamental principles of cyberattacks and also classified according to cybercrimes in Section 5. In Section 6, the various challenges of cybercrimes are discussed. Section 7 concludes this paper.

2. Cybersecurity

Cybersecurity deals with the security of the cyberspace from cybercriminals. The cyberspace constitutes all those things (hardware, software, and data/information) that are connected to the Internet/network. It is important to implement the cybersecurity effectively to protect the Internet system and the trust of people on this system from various cyberattacks. A flaw in cybersecurity and an uncovered cyberspace will provide a chance to cyberattackers to disrupt the Internet system. The three basic fundamental principles of cybersecurity are confidentiality, integrity, and availability. The three basic fundamental principles are also known as the CIA triad. The elements of the triad are considered as the most crucial components of cybersecurity [4]. The cyberattacks on the information and data on the Internet can affect these three fundamental principles of cybersecurity. So, there is a great need to setup cybersecurity to preserve these fundamental principles. Cybersecurity that does not constitute these three fundamental principles is considered to be vulnerable to cyberattacks. The fundamental principles of cybersecurity are discussed below.

2.1. Confidentiality. In the present day, every person may have confidential information like login credentials (username and password), SSN, credit card information, and a soft copy of personal documents and work files which may be stored on the computer system or server or it may be on any device connected to the Internet which needs protection from cyberattacks. Access to confidential information must be restricted to an organization of authorized users only. The measure is to be taken according to the importance of data. The higher the importance of data, the higher the risk. So, serious measures are to be taken to protect the confidential information from cyberattacks to narrow down or eliminate the risk level. There are various methods which can be used to protect the confidentiality of information from the cyberattacks:

Table 1: Classification of recent cybercrimes on the basis of security fundamental principles.

Security goals	Objective	Recent incidents of cybercrimes in 2016-17
Confidentiality	Limits the data access to authorized users only	(1) Confidential information of users of nine password manager apps like Dashlane, My Passwords, Password manager, etc. was found to be leaked. Methods used by attackers were data residue attacks and clipboard sniffing [6] (2) 85 million user accounts have been stolen from Dailymotion on 20 October 2016 [7]
Integrity	Assures the accuracy of data	(1) Cyberattack on the Ukraine Kiev's power grid caused the power outage on December 17 near midnight in the northern part [8] (2) Two weeks before the Trump's presidency in America, a cyberattacker hacked the radio stations to play "F**k Donald Trump" across the country [9]
Availability	Makes sure that authorized users always access the network and its resources	(1) Cyberattack affected 900,000 customers of Deutsche Telekom by knocking a million routers offline in November 2016 [10] (2) DDoS attacks on five major Russian banks disrupted the services of the bank to their customers for two days in November 2016 [11] (3) The WannaCry attack locked 90,000 computers in 99 countries and was ready to release them for a ransom of $300–$500 bitcoins [12]

data encryption, biometric verification, using strong user id and password, and user awareness [4, 5].

2.2. Integrity. Integrity means protecting the information and data on the Internet from alteration by cybercriminals. Integrity provides the consistency and accuracy of information on the network. The integrity of the information and data on the cyberspace can be preserved by taking appropriate steps like file permissions, user access controls, and digital signature. The bigger attacks are always the main attraction of security professionals. But security professionals cannot underestimate the small cybercrimes, as the number of small integrity attacks on information can make a huge impact on the infrastructure of an organization, state, or country. The information on the Internet might include cryptographic checksums to ensure the integrity. Backup must be maintained to recover from any tampering in information and data on the Internet due to cyberattacks or any natural calamities (earthquakes and tsunami) [4, 5].

2.3. Availability. Availability is a security policy which ensures that any individual, employee of an organization (public or private), with authorized access can use information and data on the Internet according to the specified access level by its organization. Information which cannot be used by any authorized user is like waste in a dustbin. Server systems and computer systems must have sufficient capacity to satisfy user requests for access of information on the Internet. Availability of information can be disrupted by cyberattacks, natural calamities, and environmental factors [4, 5].

Here are some latest cybercrimes that are classified according to the cybersecurity fundamental principles shown in Table 1.

3. Literature Survey

To understand a concept in a better way, it is necessary to study its pattern that can be formed by learning its past and present. This section presents the various studies related to cybersecurity and cybercrimes in different platforms from 2012 to 2016.

Liu et al. raised the need for cybersecurity in the smart grid environment [13]. They had surveys about the various factors that show that the current security mechanisms are not enough to protect the smart grids from various cyberattacks. They stated that the security requirements of smart grids are just the reverse of requirements of IT networks. They focused on the need for some different kinds of mechanism needed for smart grids that can fulfill its security requirements.

von Solms and van Niekerk presented a paper in which they explained the difference and relation between information security and cybersecurity [14]. They stated that most of the people use the term "cybersecurity" instead of information security. But both the terms have a different meaning and effect in the cyberworld. They concluded that the cybersecurity is a broader term than information security which not only provides security to a specific area but also everything that constitutes the cyberspace.

Razzaq et al. presented a survey paper on cybersecurity of data and information on the cyberspace [15]. They analyzed that nothing is safe in the present scenario. They stated that the current cybersecurity techniques are not quite efficient for all kinds of attacks and focus on the need for new security mechanisms which are not based on previous cyberattack signatures but also can defend against future attacks.

Schneider presented a paper on the need for proper implementation of cybersecurity education in educational institutions or universities [16]. He stated that the lack of the cybersecurity education in universities is giving chance to outsiders like private sector and also public sector to offer cybersecurity training which makes the work of cybercriminals easy. There is a need for study and training of cybersecurity to make an environment that can defend against cyberthreats. The devices used by a person that are connected to the Internet are difficult to hack if he/she has basic knowledge of cybersecurity. So, cybersecurity training also decreases the number of cyberattack incidents to make the work of cybercriminals harder.

Kaster and Sen presented the study of cybersecurity of the world's largest power grid [17]. From various observations, they found that the cybersecurity at the present stage is not smart enough according to new technologies and new devices that are part of the cyberworld. They presented the need and importance of cybersecurity for power grid system by pointing out that cyberthreat is the topmost threat in the list of various threats to the power grid system.

Jang-Jaccard and Nepal presented a survey on the changing trends in threats to social media, cloud computing, smartphones, and so on and various types of vulnerabilities found in hardware, software, and network infrastructure [18]. They found that the traditional approaches make the cybersecurity system stronger against existing ones and new cyberthreats are not suitable to modern technology. They stated that unique identity and the traceback techniques are new hot future research topics.

Arlitsch and Edelman presented a survey on various data breaches in 2013 and 2014 [19]. They found out that confidential data of an individual and private and public sectors are one of the main targets of a cyberattacker. Their paper focused on the need for new mechanisms to enhance the current cybersecurity for information infrastructure on the Internet.

Rawat and Bajracharya presented a survey paper on the need for cybersecurity for smart grids [20]. They discussed the increased cybersurface of smart grids and various security challenges of this extended cybersurface of smart grids. They discussed the cybersecurity attacks and defense techniques in smart grid systems that are aimed at different networks and protocol layers. Their paper is well formed to understand the concepts of the smart grid and its security.

Ali et al. presented software-defined networking as a best possible solution to enhance the security of networks [21]. They presented various benefits of using SDN (like flexible policies, threat detection and remediation, and network verification) to protect the network system from various cyberthreats. They presented some issues of SDN (NFV, overlay networks, and OpenFlow) which are yet to be resolved in the near future to protect SDN from cyberthreats. They presented the need for more advanced security for the SDN to defend against cyberattacks.

Sadeghi et al. presented the need for more security and privacy in the IoT (Internet of Things) [22]. They stated that, with the invention of new types of computing devices in the IoT environment, the attack surface has grown to be very sharp and there is a need for new security mechanisms that can cover this increased cyberspace of IoT.

Singh et al. stated that, despite several advantages of cloud computing, its one disadvantage is its major challenge in its adoption [23]. That disadvantage is its vulnerability. In this paper, they discussed a scenario of cloud computing, various security issues, and threats in cloud computing. They proposed a new 3-tier security architecture to enhance the security of cloud computing by reviewing the old techniques.

Weber and Studer presented a paper in which they showed the need, change, and importance of legal aspects of cybersecurity in the Internet of Things [24]. They stated that IoT brings a lot of advantages but whenever a new device is connected to the Internet, it also faces the same threat level which previous devices were facing. They focused on the point that the cybersecurity should not be limited to a specific point or legal aspect or regulatory approaches.

Zou et al. described the various layers of the OSI model for wireless systems which follow a different approach than wired systems [25]. They discussed the vulnerabilities of all the layers of the OSI model, and their focus is on the exploration of physical layer security concepts due to its nature of securing the open communication environment. They briefly discussed the various attacks (eavesdropping and jamming attacks) and their countermeasures on the physical layer. Their paper contributes in terms that very good knowledge of wireless security concepts and techniques used in that OSI model are explained.

As per the findings of the literature survey cited above, it is clear that cybercrimes on the Internet are an emerging and dynamic concept. The types of cybercrimes and their effects are changing day by day. However, most of the researches have discussed cybersecurity from the viewpoint of a specific environment. No general taxonomy has been provided. So, the present study is focused on the brief knowledge of cybercrimes and cyberattacks that can affect the cybersecurity in general covering various aspects of cybersecurity in terms of security principles.

4. The Proposed Taxonomy of the Cybercrime

In the existing world of Internet, we can find a huge volume and a variety of cyberattacks. From the history of cyberattacks on the Internet, it is concluded that trends of attacks are continuously changing day by day. The crime which can take place with the help of the computer system and the Internet is known as *cybercrime*. It is malicious activity which can affect the three fundamental principles of network security, that is, confidentiality, integrity, and availability. The cybercrime includes the terms like fraud, stealing, fights, and world war. These terms are also used in real-life crimes, but in the world of Internet, these terms have almost the same meaning but with different techniques. Most of the crimes occurring in today's world are cybercrimes. Hackers are finding a new way to change their attack patterns which increases the difficulty for security professionals to defend the information and data on the Internet and its resources. Hackers are providing free attack tools on the Internet to increase the number of attack rates on the Internet system. The increasing numbers of e-services like online shopping, online banking, and social apps have given a huge rise to the number of Internet users which are easily targeted by the cybercriminals. So, the various types of cybercrimes

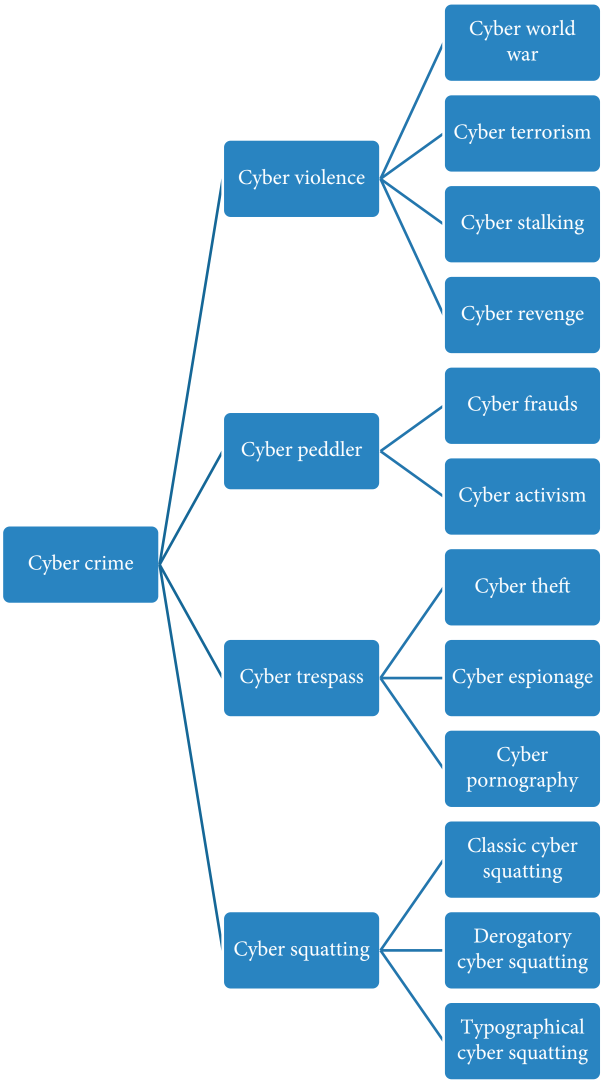

Figure 2: Taxonomy of the cybercrime.

occurring in today's world are depicted in Figure 2 and discussed below.

4.1. Cyberviolence. The violence created in real world with the help of a computer system or any device (like mobile) connected to the Internet is known as cyberviolence. Where the word "violence" is present, its effect in terms of harm will be there. In the world of cybersystem, the components that can be harmed are devices connected to the Internet, data on servers, information on the Internet, and any individual or organization that can be ruined by cyberviolence. There are various forms of cyberviolence from which most common are discussed below [26, 27].

4.1.1. Cyberworld War. The cyberworld war has a maximum level of violence that acts among various countries of the world. The cyberworld war constitutes every individual, military, country, hackers, and government and private employees. The aim of the cyberworld war is to malfunction, to disable, or to destroy the infrastructure and resources based on the Internet system of rival or enemy country. In this war, every type of cyberattack is used to achieve victory over the target country.

4.1.2. Cyberterrorism. There are some people or groups which have only aim of destroying the humanity known as terrorists. They believe that they are doing this to make their religion more powerful in the world or they have only right to command over the world or no other can be stronger than them. The terrorism like this in the digital world is known as cyberterrorism. They have no emotions or sympathy. They are like machines whose aim is fed into them. They can use any type of cyberattack to fulfill their aim.

4.1.3. Cyberstalking. It is like for loop of C language in which termination condition is the harassment of your target. In this type of attack, attackers make use of electronic communication (email and instant messaging) to attack their target [28].

4.1.4. Cyberrevenge. Revenge means harming someone in response to one's previous action. The aim of cyberrevenge is to destroy the enemy by various ways like exposing their confidential information, destroying their computer-based infrastructure and resources, and making their false image on the Internet system. The aim of cyberrevenge is to steal and change the confidential information of enemy for his/her vested interests.

4.2. Cyberpeddler. Cyberpeddler is an act of doing something illegal or stealing someone's confidential data with the help of a computer system connected to the Internet. There are basically two types of cybercrimes in this category which are discussed below.

4.2.1. Cyberfraud. The act of making financial or personal gain by deception is known as cyberfraud. The main aim of fraud is to gain benefits in terms of money. Cyberfrauds include social engineering attacks like password guessing, spear phishing, and DNS redirecting in which the hacker manipulates the users to get their confidential information and then uses this information for his/her vested interests.

4.2.2. Cyberactivism. It is the latest type of crime. In this type of crime, Internet-based social and communication applications are used to create, operate, and manage the activism like faster communication with people or the distribution of information to a large audience in a few seconds. The communication technologies used in this activism are Twitter, Facebook, YouTube, LinkedIn, Whatsapp, Gmail, and so on. These technologies are made for good purposes like better connectivity with friends, colleagues, and employees and spreading the latest information easily to a vast geographical area. But some people use these technologies for spreading rumours to damage their rival image or spread false information about their organization or individuals to get various types of benefits [5].

4.3. Cybertrespass. Trespass means crossing boundaries for which someone is not authorized. Cybertrespass is the crime in which cyberlaw is violated by hacking an authorized user system. This type of attack violates the confidentiality and integrity fundamental of cybersecurity. The various types of cybertrespass are as follows [26, 27].

4.3.1. Cybertheft. Theft means there is a fear of something important that can be damaged or stolen. In real life, stealing or damaging is done by going physically into someone's house or organization and stealing something like file, television, gold, and so on. But in case of cyberworld, it is different from real world. Cybertheft in the cyberspace can be done by technically hacking someone's computer system connected to the Internet. In cyberworld, hackers have the aim of stealing/damaging information and data on the cyberspace for financial or personal gain. Basically, there are two types of thefts:

(i) Theft to cyberspace: Space is one of the important factors, which if not maintained properly leads to malfunction of the Internet. Cyberattackers aim to overflow the cyberspace to stop their target services or hack their targets.

(ii) Theft to data/information: Data/information constitutes the confidential record of an individual, organization, and country. The confidentiality, integrity, and availability of information on the Internet and servers must be maintained from cyberattackers.

4.3.2. Cyberespionage. It is also known as cyberspying. It is the act of tracking the activity of individual, company, organization, country, enemy, or rival by performing malicious activities on the network. These are technically sound people who are difficult to detect. They analyze the network traffic illegally, or they can hack the security cameras and laptop cameras to obtain the information about their targets, that is, what type of information they are accessing, what type of work they are doing, and when they leave their workplace or home [5].

4.3.3. Cyberpornography. It is the attack in which an attacker posts sexual or nude material of his/her target on public websites. The attacker can find the private material of his/her target by hacking the target computer system, mobile, security cameras, or tablet. This type of exposure of private pictures or videos makes shame to the target of the attacker, or even in some cases, the target commits suicide [26, 27].

4.4. Cybersquatting. It is the cybercrime in which an attacker illegally registers the name of the trademark of others as domain name so that the owner of the trademark fails to register his/her trademark as domain name. The various types of cybersquatting are discussed below [29].

4.4.1. Classic Cybersquatting. It is the same as cybersquatting, but the main aim of the cybersquatter is to get paid. When the cybersquatter gets ransom from his/her target, he/she sells off or deletes his/her domain name. But now, laws have been changed, so the trend of this type of attack is not very popular today [29].

4.4.2. Derogatory Cybersquatting. In this type, the cybersquatter's main aim is to destroy the reputation of his/her target. A cybersquatter does this by various means like posting the pornographic material, hate speech, or violated contents on that domain name [29].

4.4.3. Typographical Cybersquatting. In this type of attack, the attacker cannot use the same name as the trademark because the owner of the trademark had already registered for the domain name. So, in this case, the attacker registers with the name very similar to the original trademark name. For example, if the attacker registers a domain name of Gmail that is very similar to Gmail, then he/she may succeed to make loss to the original trademark owner [29].

Figure 2 represents the major categories of cybercrimes happening in today's world. According to us, any kind of cybercrime can be subcategorised in this taxonomy. Our taxonomy helps a reader to easily understand the similarities between the attacks.

5. Classification of Cyberattacks on the Basis of Fundamental Principles of Cybersecurity

Cyberattacks are the techniques used by cybercriminals to disrupt the fundamental principles (confidentiality, integrity, and availability) of cybersecurity. Cyberattacks are skills of a cyberattacker to do cybercrimes in the Internet system. Cybercrimes present the general form, whereas cyberattacks are the specific form of attacks/crimes on cybersecurity. Here, we will discuss the cyberattacks on the cybersecurity fundamental principles as shown in Figure 3.

5.1. Attacks on Confidentiality. It is detected that there are many kinds of attacks on confidentiality of network information which are as follows.

5.1.1. Traffic Analysis. In the traffic analysis attack, an attacker analyzes the information on the network between the sender and the receiver without any tampering in it. The attacker makes analysis of information on the network to find some new information to steal confidential information. It is a passive attack, and it only violates the confidentiality principle of network security [30].

5.1.2. Eavesdropping. Eavesdropping means secretly listening to a confidential conversation on the network. An

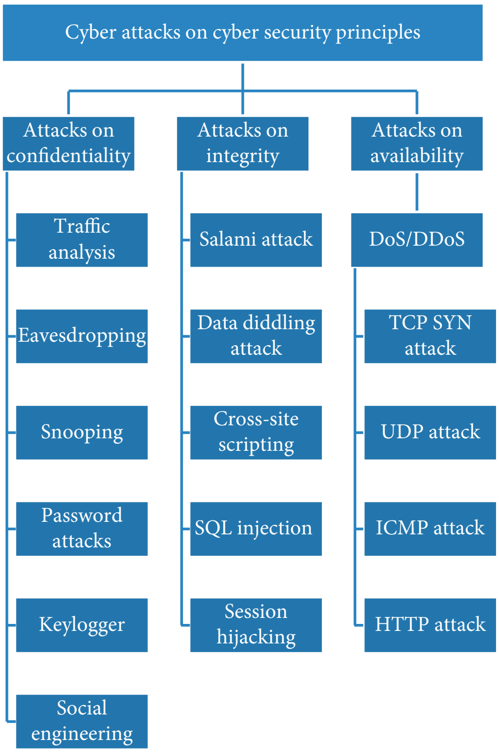

Figure 3: Classification of cyberattacks on the basis of fundamental principles of cybersecurity.

attacker can read and capture the information on the network between the sender and the receiver. This attack is similar to traffic analysis. But in this type of attack, an attacker can sniff and record the information and later listen or read this information for his/her vested interests [31].

5.1.3. Snooping. It is the passive form of attack where the attackers attempt to obtain confidential information about network users like login credentials of email, social apps, online banking, and so on or their personal records. The corporate sector or government officials use the snooping method to track their employees' activities for various purposes. Snooping is further divided into two types as discussed below [5].

(i) Digital snooping: Monitoring a private or public network for passwords or data is known as digital snooping. This attack is performed at the network layer. This snooping is done on the physical cable. Attackers may reprogram network switches or other devices to allow them to capture data off a network. Attackers can hack security cameras of an organization to get the username and password of employees so that they can access organization data like authorized users [5].

(ii) Shoulder snooping: This is a physical attack where someone tries to watch for typed passwords or see information on a monitor that they should not have access to [5].

5.1.4. Password Attacks. Password-based attacks are used to get the username and password of authorized users of an application, website, desktop computers, and laptops. These captured usernames and passwords are further used to get access to network services as authorized users and to do malicious act. The success of password attacks depends upon the user awareness on how to choose the password. If the user is aware about choosing passwords, it will add complexity for hackers to gain access to the authorized user's password. There are various types of password attacks as discussed below.

(i) Dictionary-based attack: In this attack, an attacker tries every combination of characters or words as defined in the dictionary to hack passwords of authorized users of Internet resources or applications. This type of attack result depends on the authorized user's password. If the user does not choose passwords similar to dictionary words, then it is almost impossible for the attacker to hack the password of the user with this attack.

(ii) Brute-force attack: In this attack, an attacker tries every single possible password combination using brute-force hacking tools to hack the user password. This technique is time-consuming but results in the hacking of the authorized user's password. This attack can take few seconds to few days or few months also according to the complexity of passwords.

(iii) Password-guessing attack: In the password-guessing attack, an attacker tries to guess the passwords of authorized users by using common words like date of birth, name, and religion.

5.1.5. Keylogger. Keylogger is a type of malware that runs in the background of a computer system in the hidden mode; that is, the user is not aware about the running of keylogger. It has no icon or entry on desktop, quick launch, all programs, or anywhere else in the computer system. All the information entered by the user is captured by keylogger and transmitted to the attacker without the knowledge of the authorized user of that computer system [32].

5.1.6. Social Engineering. Social engineering is a type of attack in which someone with very good interactive skills manipulates others into revealing information about the network that can be used to steal data of authorized users of an organization or an individual. Attackers carry out this attack by either influencing network users or through technical attack. It aims at small groups of Internet users. The various types of social engineering attacks are discussed below [33].

(i) Phishing: Phishing is an attempt to hack sensitive information (usually financial information like bank user id/password, credit card details, etc.) of network users by tricking them in various forms. These attacks use fake emails and websites which look almost the same as the original to fool the people. It aims at small groups to large groups of network users. The various types of phishing attacks are discussed below [34].

(a) DNS phishing: DNS phishing is a process in which an attacker alters host files on the victim's computer system or DNS database or at any access point so that legitimate web URLs point to a fraudulent URL of the attacker. Due to lack of awareness about phishing attacks, users enter their confidential information in the fraudulent website of the hacker. Sometimes, technically sound people also fail to differentiate between the fraudulent website and the authorized website [34].

(b) Spear phishing: It is a form of targeted attacks. At first, an attacker seeks available public information of its target through websites or social networking sites. On the basis of public information gathered, the attacker makes malware-contained email to gain the victim trust. Then, the attacker sends this email to some selected people whom he/she wants to target. If anyone receiving that email clicks on it, he/she will become the victim of the attacker and lose his/her confidential information to the attacker because the malware attached with email works automatically when email is opened [33].

(ii) Dumpster diving: It is an attack in which an attacker himself/herself finds confidential information of a network user or an organization without the use of the network system. For example, the attacker may look up trash of an organization to find sensitive information [33].

(iii) Baiting attack: In this approach, an attacker places the malware-infected storage device (CD, DVD, and pen drive) at that point where the future victim may see that device. The attacker adds more curiosity to the victim by labelling that storage device. When a person uses that storage media, his/her computer system gets infected and he/she will become a victim of the attacker's attack [33].

(iv) Waterholing: It is a form of targeted attack in which an attacker indirectly targets his/her victim. In this method, the attacker infects those websites which his/her target mostly visits so that the victim computer system may get affected and the attacker gains access to his/her confidential information [33].

(v) Reverse social engineering: In this attack, an attacker represents himself/herself as a trusted person to the victim. Then, the attacker creates a situation in which the victim believes that the attacker is a person who can solve his/her problem and trustworthy to share his/her confidential information [33].

5.2. Attacks on Integrity.

A huge number of attacks can be found to disrupt the integrity of network information which are as follows.

5.2.1. Salami Attacks.

Salami attacks are a series of minor data security attacks that together result in a larger attack. Example of this attack is a deduction of very small amount of money from bank account which is not noticeable. But when these deductions of very small amount from various numbers of accounts in the bank become a huge amount, it can damage the infrastructure of the bank [35].

5.2.2. Data Diddling Attacks.

Data diddling is an illegal or unauthorized data alteration. For example, account executives can change the employee time sheet information of employees before entering to the HR payroll application [35].

5.2.3. Cross-Site Scripting (XSS).

In this attack, an attacker uses vulnerable websites or applications. The hacker inserts his/her malicious script into that website or application that a target user visits. When the target visits that vulnerable website, the hacker's malicious code is transferred to the victim's browser. This malicious script can access sensitive information like cookies and session from the victim's browser [36, 37].

5.2.4. SQL Injection Attack.

It is also an injection attack like cross-site scripting. But this attack uses the vulnerabilities of database SQL statements. This attack affects the web application database. It also affects websites and web applications that make use of databases. The attacker can gain access to the sensitive information of the database by bypassing the web application's authentication and authorization mechanism [36, 38].

5.2.5. Session Hijacking Attacks.

Session hijacking is another type of network attack where the attacker alters session between two or more authorized users to gain authorized access to information or services used by authorized users. TCP session hijacking and man-in-the-middle attacks are examples of this type of attack [35].

5.3. Attacks on Availability.

There are various methods that can be used to slow down or stop the availability of network resources to the authorized users of the Internet and its resources. Here are a few common attacks against availability that are discussed below.

5.3.1. DoS/DDoS.

DoS (denial of service) is a very common attack that disrupts the availability of the network and its resources. An attacker can attack his/her target directly or indirectly or both. In direct attack, the attacker generates huge traffic by using his/her own computer system, and in indirect attack, the attacker uses bots (a system that is hacked by an attacker and is under his/her control) to generate huge traffic for his/her target. A large variant of the DoS attack is DDoS (distributed denial-of-service) attack in which a number of bots or even a server can be used to make an attack on the target to disrupt his/her network services.

Table 2: Classification of cyberattacks on the basis of cybercrimes.

Cyberviolence	Cyberpeddler	Cybertrespass	Cybersquatting
Denial of service/distributed denial of service	Keylogger and social engineering	Traffic analysis, eavesdropping, snooping, password attacks, SQL injection, salami attack, and data diddling	Session hijacking

DoS/DDoS attack can disrupt the network bandwidth, system resources, and application resources [39].

The consequences of a DoS attack are the following:

(i) Slow network performance

(ii) Unavailability of network services

The various types of Dos/DDoS attacks are discussed below.

(i) TCP SYN attack: In this type of attack, an attacker uses the flaw of the three-way handshake process during TCP (transmission control protocol) connection establishment. In the three-way handshake process, the client sends SYN (synchronization) request to the server. Then, in the second step, ACK (acknowledgement) is given by the server with SYN to the client. At the last step, the client sends the final ACK. The attacker sends too many SYN requests and never gives the final-step ACK which overflow the target capacity of request handling or memory which results in nonavailability of network services. The attacker can also use spoofed address to send requests so he/she does not get any response from his/her target which can also overwhelm his/her network [40].

(ii) UDP attack: TCP is the connection-oriented protocol and UDP (user datagram protocol) is the connectionless protocol, and both work on the transport layer of the TCP/IP model. The connectionless mechanism used packets for information exchange and is used where reliability can be compromised up to some extent. An attacker generates huge traffic of UDP packets to his/her target to overflow his/her response handling queue which results in nonavailability of network services to authorized users [40].

(iii) ICMP attack: ICMP (internet control message protocol) works on the network layer of the TCP/IP model. It is used by network devices (like routers) to generate an error report when there is problem in the delivery of IP packets. An attacker generates and sends a huge volume of ICMP traffic to the target host which will consume the bandwidth of the target network. ICMP can be performed by two ways, that is, ping of death and smurf attacks, discussed below [41].

(a) Ping of death attack: Ping is a mechanism used to check the availability of a particular IP address by using small packets. An attacker sends large-sized packets in a ping which has a range higher than the maximum limit of packet size that TCP/IP allows. So, the target is not configured for these large-sized packets because it may crash, freeze, or reboot [42].

(b) Smurf attack: Smurf attack basically uses the amplification approach. It targets the Internet broadcast address (IBA) that is built in the IP protocol. A hacker sends request by generating ICMP traffic with spoofed address (containing address of the target) to IBA of the intermediary site that will generate and send amplified response to the target host. All this process works on the network layer of the TCP/IP model, but the intermediary response is sent to all hosts on layer 2. An IBA can support a maximum of 255 hosts. So, a smurf attack amplifies a single ping 255 times [40, 43].

(iv) HTTP attack: HTTP (Hypertext Transfer Protocol) works on the application layer of the TCP/IP model. It targets all the web applications and services which use HTTP packets (GET and POST requests). This type of attack does not need high volume of traffic, so this attack needs less bandwidth. In this attack, an attacker sends a large volume of GET or POST requests to the target which results in overwhelm of target capabilities [40, 44].

Table 2 represents the various types of cyberattacks grouped on the basis of cybercrime categories. According to us, every type of cyberattack can be adjusted in Table 2. Our cybercrime taxonomy gives a way to uniquely distribute the cyberattacks. It helps to understand the similarity and differences between various types of cyberattacks. Table 2 helps the newcomers to decide what type of security technique is effective on what type of cyberattacks. Hence, classification of cyberattacks according to cybercrime categories in Table 2 provides a complete understanding of common types of cyberattacks. So, a security technique can be updated to protect the cyberspace from more than one cyberattack.

6. Challenges to Tackle Cybercrimes

The increasing technology of the Internet has provided various advancements in human beings' daily life. But this advancement of technology is facing various challenges that are discussed below.

6.1. Mixed Attacks. Various mechanisms are discovered by cybersecurity researchers to defend against cyberattacks. But there is no such single technique that can defend the data and information on the Internet from all the cybercrimes. Cybercriminals are very creative. They are always busy in making a new variant of existing cyberattack or forming a new cyberattack. This type of dynamic environment of cybercrimes gives a very hard challenge for security researchers to defend the data and information on the Internet from the various types of cyberattacks from cyberattackers [25].

6.2. Huge Increase in the Cybersurface. The increasing popularity of the Internet has given a steep rise to the cybersurface. The cybersurface basically constitutes desktops, laptops, mobiles, tablets, and smartwatches that can be connected to the Internet with the help of hardware and software. The Internet of Things (IoT) and cloud computing are major platforms that have extended the cybersurface to a large circumference as stated in [3]. The increased cybersurface provides various opportunities to cybercriminals for cyberattacks due to lack of proper implementation of cybersecurity. Some vendors have major focus on their product's quality and minor on cybersecurity. They do not implement the full-fledged cybersecurity mechanisms which give opportunities to the cyberattacker to enter an Internet or network system like an authenticated user. This increased cybersurface gives rise to the difficult level of defending data on the cybersurface by security professionals. Some new type of security standards is needed to implement properly the cybersecurity to save the cyberspace from cybercriminals [24].

6.3. Remote User Connectivity. In the present stage, government and private sectors have offered an opportunity to its employees to connect remotely from anywhere by deploying the Internet-based virtual private network (VPN). This facility has enhanced the working system of these sectors. But this system has brought the private information of these sectors to public networks. Remote user connectivity also provides opportunities for cybercriminals to hack the Internet-connected devices remotely. There is a challenge for network security professionals to provide security from cybercriminals to the corporate or government sectors' confidential information on public networks and those public devices who have such confidential information [45].

6.4. Network IP Address Infrastructure. The numbers of Internet-connected devices are proportionally larger than the numbers of Internet users as stated in [3]. A single user of the Internet can have a mobile, a laptop, or a desktop. Each device has a unique IP address on the Internet. The traditional methods of manually configuring IP addresses are no longer viable, and they also lack the scalability, reliability, and effectiveness of security methods needed by the today's networks. So, securely and effectively managing the IP addresses of these fast-growing networks is a big challenge for a network administrator as the forged IP address is used by the cyberattacker to disrupt the Internet system [45].

6.5. Unified Network Control. The technique SDN (software-defined networking) is widely adopted to control the Internet system easily and effectively than the traditional system. This technique provides various benefits like the centralized network approach, low cost, and reliability. But the flaws in this technique have provided various opportunities for cybercriminals to hack the control of the network system. If security of the controller working in the control plane of SDN is compromised, then the complete architecture of the network system will be compromised where the SDN is installed. This will give the confidential information of many users, the control of various networking devices, and the integrity of applications installed on that network to cybercriminals. So, this is a big challenge for security professionals to protect the SDN from cybercriminals [21].

6.6. One Technique for All Layers. There are different techniques to protect all the layers of the OSI or TCP model. It is a complex task to advance all the techniques according to the latest cyberattacks at a time. It is also wastage of time and money to make many techniques for the previous known attacks. There is a need for a single technique that should protect all the layers of the ISO or TCP model from various known and unknown cyberattacks [25].

7. Conclusion

The increasing popularity of the Internet has given a sharp rise to the digital world which constitutes very large volume of information and data stored on the cyberspace. With the increase in cyberspace, the cyberattacks/cybercrimes are also increasing in numbers and their effect is also growing bigger. The existing security techniques are not enough to protect the current Internet system and its resources. Some new types of security techniques are required to defend the cyber space from cybercrimes that can never be cracked or require years to crack down, which are cost-effective and can defend against all types of cybercrimes. We cannot misguide the cybersecurity as information security or data security. Cybersecurity is a broader term which protects all the hardware (devices, routers, and switches), software, information, and data that are part of the Internet. On behalf of our study, the future work will constitute the following points:

(i) To propose a security technique that can defend against ever-changing attacks at different levels of network protocols

(ii) To propose an effective, accurate, and cost-efficient security technique for a specific environment (IoT, cloud computing, SDN, and smart grid)

(iii) To propose a technique for securing the information in remote user connectivity or BYOD (Bring Your Own Device) policy

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] March 2017, https://wearesocial.com/special-reports/digital-in-2017-global-overview.

[2] March 2017, http://www.gartner.com/newsroom/id/3165317.

[3] *Report of McAfee Labs 2016 Threat Predictions by Intel Security*, November 2016.

[4] M. Haughn and S. Gibilisco, *Confidentiality, Integrity, and Availability (CIA Triad)*, March 2017, http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[5] G. Kumar, A. Kaur, and S. Sethi, "Computer network attacks-a study," *International Journal of Computer Science and Mobile Applications*, vol. 2, no. 11, pp. 24–32, 2014.

[6] April 2017, http://thehackernews.com/2017/02/password-manager-apps.html.

[7] April 2017, http://thehackernews.com/2016/12/dailymotion-video-hacked.html.

[8] April 2017, http://thehackernews.com/2016/12/power-outage-ukraine.html.

[9] April 2017, http://thehackernews.com/2017/02/radio-station-trump-hack.html.

[10] April 2017, http://thehackernews.com/2016/11/mirai-router-offline.html.

[11] April 2017, http://thehackernews.com/2016/11/bank-ddos-attack.html.

[12] April 2017, http://thehackernews.com/2017/05/how-to-wannacry-ransomware.html.

[13] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Philip Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[14] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013.

[15] A. Razzaq, A. Hur, H. Farooq Ahmad, and M. Masood, "Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, pp. 1–6, Mexico City, Mexico, March 2013.

[16] F. B. Schneider, "Cybersecurity education in universities," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 3-4, 2013.

[17] P. Kaster and P. K. Sen, "Power grid cyber security: challenges and impacts," in *Proceedings of the 2014 North American Power Symposium (NAPS)*, pp. 1–6, Pullman, WA, USA, September 2014.

[18] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[19] K. Arlitsch and A. Edelman, "Staying safe: cyber security for people and organizations," *Journal of Library Administration*, vol. 54, no. 1, pp. 46–56, 2014.

[20] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: status, challenges and perspectives," in *Proceedings of the SoutheastCon 2015*, pp. 1–6, Fort Lauderdale, FL, USA, April 2015.

[21] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A survey of securing networks using software defined networking," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1086–1097, 2015.

[22] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, San Francisco, CA, USA, June 2015.

[23] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[24] S. H. Weber and E. Studer, "Cybersecurity in the internet of things: legal aspects," *Computer Law & Security Review*, vol. 32, no. 5, pp. 715–728, 2016.

[25] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[26] M. Yar, *Cybercrime and Society*, SAGE Publications, Thousand Oaks, CA, USA, 2013.

[27] D. Wall, *Crime and the Internet*, Routledge, Abingdon, UK, 2003.

[28] April 2017, http://searchsecurity.techtarget.com/definition/cyberstalking.

[29] N. S. Sreenivasulu, *Law Relating to Intellectual Property*, Partridge Publishing, Gurugram, India, 2013.

[30] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[31] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[32] A. Solairaj, "Keyloggers software detection techniques," in *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1–6, Coimbatore, India, January 2016.

[33] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.

[34] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, "Phishing attacks and defenses," *International Journal of Security and Its Applications*, vol. 10, no. 1, pp. 247–256, 2016.

[35] April 2017, http://www.omnisecu.com/ccna-security/types-of-network-attacks.php.

[36] A. Kieyzun, P. J. Guo, K. Jayaraman, and M. D. Ernst, "Automatic creation of SQL injection and cross-site scripting attacks," in *Proceedings of the 31st International Conference on Software Engineering (ICSE 2009)*, pp. 199–209, Vancouver, BC, Canada, May 2009.

[37] April 2017, https://www.acunetix.com/websitesecurity/cross-site-scripting/.

[38] April 2017, https://www.acunetix.com/websitesecurity/sql-injection/.

[39] V. Zlomislic, K. Fertalj, and V. Sruk, "Denial of service attacks: an overview," in *Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, Barcelona, Spain, June 2014.

[40] O. Osanaiye, K.-K. Raymond Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147–165, 2016.

[41] April 2017, http://www.webopedia.com/TERM/I/ICMP.html.

[42] April 2017, http://searchnetworking.techtarget.com/definition/ping.

[43] April 2017, http://www.techrepublic.com/article/understanding-a-smurf-attack-is-the-first-step-toward-thwarting-one/.

[44] April 2017, https://www.verisign.com/en_US/security-services/ddos-protection/ddos-attack/index.xhtml.

[45] S. Barnett, "Top 10 challenges to securing a network," *Network Security*, vol. 2000, no. 1, pp. 14–16, 2016.