A REVIEW: IMPORTANCE OF CYBER SECURITY AND ITS CHALLENGES TO VARIOUS DOMAINS

Chalsi Sharma[1], Satish Maurya[2]
E-Mail Id: [1]sharmachalsi24@gmail.com, [2] mauryasatish855@gmail.com
Manav Rachna International Institute of Research and University, Delhi, India

Abstract- Cyber security means being in a state of security from the vulnerabilities available in the network. Being in a world, where millions and trillions of systems are interconnected, it is quite important to save our precious data from cyber-attacks. This paper focusses on the cyber security trends and corresponding challenges.
Keywords-Cyber Security, Cyber-Attacks, Vulnerabilities, Cyber Threats.

1. INTRODUCTION

Cyber threats have become a common problem in computer devices. Because ensuring cyber security prevents our devices from cyber-attacks and from being hunt in a cybercrime. As cyber-crime is increasing every individual should aware of the cyber security of their devices. Today, the infrastructure of the internet is evolving and changing day by day with emerging new technologies. Even with new technologies cyber threats are also increasing and challenging the security of devices. Technologies that are trending these days like cloud computing, social networking, E-commerce also facing problems of lacking security.
The major parts and infrastructure of cyber security as follows: -

2. CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (CIA)

CIA stands for Confidentiality, Integrity, and Availability.

2.1 Confidentiality

The state of keeping private. The main objective of confidentiality is to protect sensitive information from reaching the wrong people. Solution- Data encryption is a common method to ensure confidentiality. There are two types of data encryption –

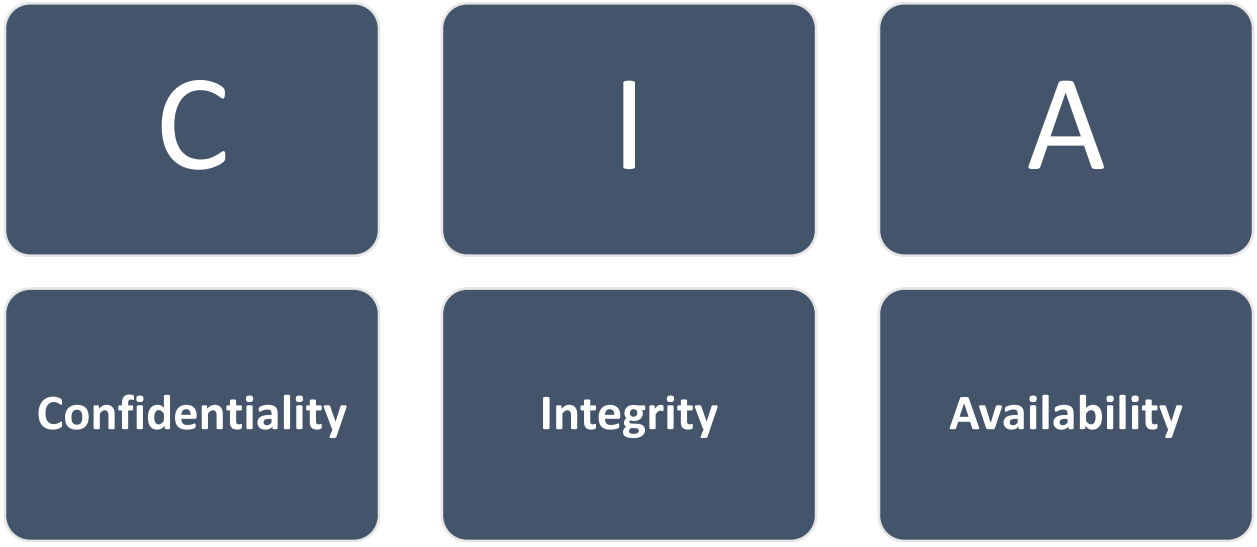

Fig. 2.1 The CIA Triad

2.2 Asymmetric Encryption

Public key encryption is used in asymmetric encryption. It is a combination of two keys. One key encrypts only and the other one decrypts. E.g. - If Sam sends any messages only Alice can decrypt it and if Alice sends a message only Sam can decrypt it.

2.3 Symmetric Encryption

It is a type of encryption where only one key is used to both encrypt and decrypt. Both the parties should exchange their keys.

2.4 Integrity

Accuracy and trustworthiness of data. Its main motive is to prevent the altering of data by an unauthorized person. Solution- Backups and redundancies must help to restore the affected data to its previous state and confidentiality also helps in providing integrity.

2.5 Availability

Available to authorized users only i.e. Data and information are only accessed by authorized personalities. To maintain availability, we ensure all software updates and all software and hardware are working properly.

3. CYBER ETHICS

It is defined as the relationship between computer and society i.e. how a computer used to affect the society and its impact on the world. There are also a lot of rules and regulations a user should keep in mind while using a computer or internet that is also called cyber laws. To ensure cyber ethics a user should keep these few points in mind. [3] –

- The user should not operate other accounts using their passwords [10].
- The user should not send any kind of malware to anyone using the internet.
- Always use copy-righted software and games etc.
- Never use pirated content.

3.1 Internet Hacking

Hackers are those who use computers to gain unauthorized information or data. Since the world is full of computers so it is important to prevent them. Hackers mainly inject some viruses in the device and affect them. [4]
To prevent a device from a hacker, keep these points in mind –

- Keep updated OS and software frequently. If there is any hardware problem repair it immediately.
- Download a security program such as anti-virus to protect system from viruses.
- Don’t save passwords in any device or never share your passwords with anyone.
- Keep all your sensitive data on the cloud.
- Don’t use unknown Wi-Fi or never provide an unknown person your device hotspot.

3.2 White Hat Hacking

White hat hackers (also known as Ethical Hackers) are idioms used to explain that hackers are the ultimate security professional where they work under a person or a company to find and exploit vulnerabilities and weaknesses in various systems - they also help people by identifying potential threats to a device.An ethical hacker (or white-hat hacker) performs a role similar to that of a penetration tester, involving major responsibilities/ duties. They break into systems legally and ethically.
It is considered legal because it used to ensure the security of a device. [5]

4. PHRASEOLOGY OF CYBER SECURITY

There is some major realm which cyber security includes in it:

4.1 Application Service Provider

Application security/service provider is an enterprise that delivers application functionality and associated services across a network to multiple customers using a rental or usage-based transaction-pricing model. Application security is the process of developing, adding, and testing security features within the applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
Whenever a software is created the user needs their software to be protected. Application security encloses evaluate or countermeasures the threats that can enter a software through an inadequacy or a fault in designing an application or in any up gradation or maintaining any of the application software and protects the application during the organization's life cycle.
Application security may include hardware, software, and procedures that identify or minimize security. Different types of application security features include authentication, authorization, encryption, logging, firewalls, antivirus programs, encoding programs, and application security testing which can be used to prevent unauthorized access.

4.2 Documentation Retrieval

Information security is the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.
The process, tools, and strategy need to prevent documents deleted, non-digital information and counter-threats are needed to be managed by a set of strategies or approaches known as Information Security.

Information security management programs are taken into consideration and are built around the objectives like it declares and it also explains the responsibilities which a company requires to implement to protect confidentiality (the information does not get disclosed to the unauthorized parties), availability (it is an argument that provides us the information about a given data could be easily accessed when requested by the authorized parties, no unauthorized party can access it) and integrity(prevention of modification of data in and unauthorized way) of assets from threats and vulnerabilities[2].

4.3 E-mail Security

E-mail is one of the most widely used features of the internet, along with the web. It allows you to send and receive messages to and from anyone with an email address, anywhere in the world. Today email supports HTML, which allows emails to be formatted the same way as websites. There are some main activities through emails - we can attach files along with the messages, user can store the information.

An email is a digital message sent electronically from one computer to one or more other devices. So, hackers/ attackers can hack or manipulate a person's sensitive or personal information.

As emails are flexible and can be used for giving instructions, serving as documentation, providing confirmation, communicating rules and procedures. Therefore, email has become a usual platform for the attackers to hold a network of sensitive information and the most important organization's data.

Securing an email needs an application that could block the incoming attacks through various, methods for maintaining the record of personal and sensitive information by controlling outbound messages and maintaining a secure wall between the user's information and unauthorized access from the attackers to avoid any loss.

4.4 Insecurity of Digital Devices

4.4.1 Data Leakage

Prevention of this problem permit only some apps to access your location or contracts which require them on a necessary basis. Because today most of the transactions being done online through the internet and if someone got your account details and pin can easily make a fraud by using it.

4.4.2 Unsecured Wi-Fi

In and of itself, a wireless access point (WAP) or wireless network connection isn't inherently dangerous. It becomes so if it's unsecured - allowing the movement of data across its airwaves without any form of encryption or security protection. To be safe from such threats, use free Wi-Fi on your device and never allow it to access your confidential or personal information like credit card or online transaction passwords etc. which are more than personal for a person.

4.4.3 IP Spoofing

Attackers may use IP (Internet Protocol) spoofing to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address spoofing is to gain access to networks that authenticate users based on IP addresses.

To be safe, log in with a unique password and never provide personal information while using free Wi-Fi.

4.4.4 Malware

Spyware (type of Malware) is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware - malicious software designed to gain access or to damage your computer, often without your knowledge.

Installing a strong anti-virus and malware detector is the best way to secure your computing devices as they will delete the programs in your system before they can access and collect your sensitive data.

4.5 Internet Security

An example of internet security is an online system that prevents credit card numbers from being stolen on a shopping website.

It is a branch of computer security specifically related to not only the internet, often involving browser security on as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the internet.

4.6 AF-FM Security

AF-FM (or Wireless) security is used to prevent the damage or unauthorized access to computers. It also protects data & wireless networks, which include Wi-Fi networks. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer the key length improves over WEP (Wired Equivalent Privacy).

If we don't take some special measures like downloading and installing a wireless LAN then our wireless networks are still unsafe like our wired networks

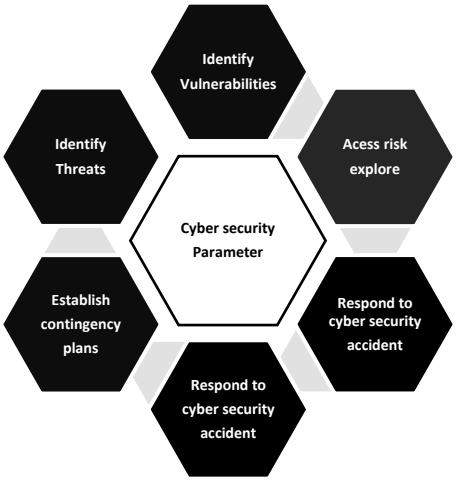

Fig 2 shows Cyber Security Parameters

5. SECURITY ATTACKS, ITS TYPES & SOLUTIONS

An attempt to gain unauthorized access to information resources or services, or to cause harm or damage to information systems is known to be Security Attacks.
Let's take a look at what those concerns are, their solutions: [3]: -

5.1 Denial of Service Attacks

This type of attack concerns with the multiple systems when they flood the bandwidth of the system which it attacks. The system or a network shut downs in result of this attack which makes it inaccessible to the users. This type of attack is detected by monitoring the network traffic using a firewall or any detection system, it can also be prevented by limiting the number of requests to a server in use.

5.2 Exhaustive Search Attack

This attack is really concerning as it includes the attackers submitting various passwords or usernames ultimately getting one as a correct password. This happens as the attacker systematically monitors all the passwords possible and checks it until the correct one is found. To prevent such attacks, Administrator must ban using some popular passwords and he/she must use the most unpredictable passwords.

5.3 Portal Attacks

This type of attacks allows an attacker to interfere in the information sent from user's browser to server, and works regardless of existence of multiple web application. Such attacks are carried out in an attempt to steal financial information by intercepting a user's traffic to a banking life.

5.4 Shell Shock Attacks

This assault is a bug that uses a vulnerability in the common UNIX command execution shell bash (Bourne-Again Shell) to potentially enable hackers to take control of the machine and remotely execute code directly into the system.

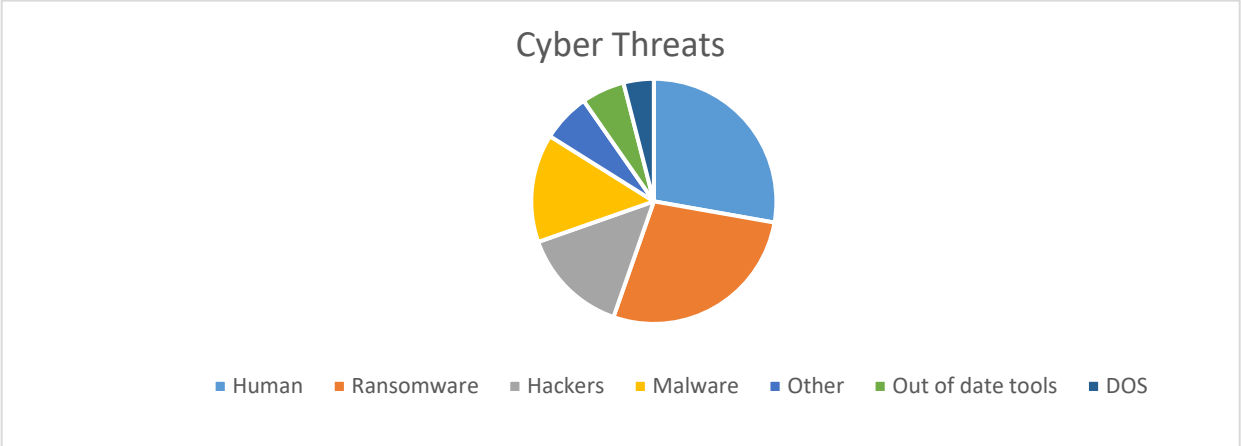

Fig. 5.1 Percentage Ratio of Cyber Threats [2019]

6. CHALLENGES TO CYBER SECURITY

6.1 Evolving Technologies

With the increasing technology attackers have also evolved a lot of ways to break the security of the system. Now plenty of methods or ways by which they can try to access a device. In 2019 there are a lot of ways by which a hacker can exploit any device if the device has poor cyber security. So that's why we need to keep our devices fully secure from them.

6.2 Lack of Architecture of Cyber Security & Awareness

A lot of countries still have poor Cyber security due to poor cyber security architecture that's why attackers can easily damage and corrupting their data lead to cyber-crimes. There are a lot of countries having poor literacy rates and if we talk about cyber security people know very less about it. Not only people but also teachers who are teaching cyber security are not well updated about today's trends in cyber security so, that's why it's too important to be updated. Hackers always use different tactics to break the security of a device.

6.3 International Challenges to Cyber Security

We aren't aware sufficiently and as individuals, we are not prepared, cyberspace being the main threat to the nations on the international community. Despite the growing no. of users, the internet provided still beyond or below minimum ordinance. Those are the main reason and conditions for the establishment and recognition of the actions taken in the name of cyberspace.

Cyberspace is representing the security risk and challenge of modern time. The development and application of information and communication technology has created a new field of battleground. As a special challenge to international security, cyber terrorism arises. Cyber security will significantly affect international relations in the 21st century [4].

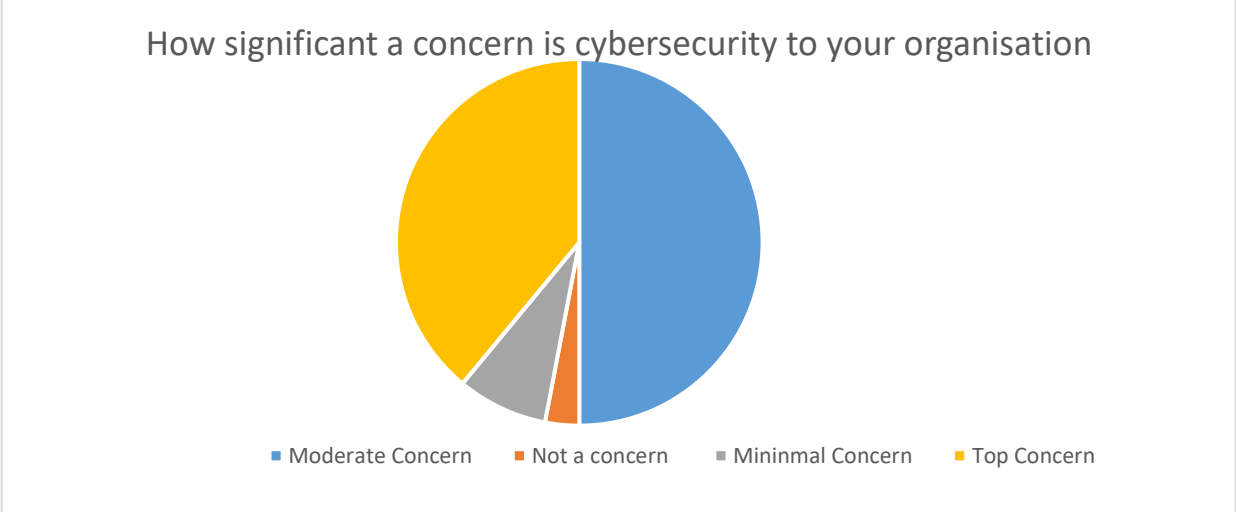

Fig. 6.1 Percentage Cyber Security Concern [12]

7. ROLE OF SOCIAL MEDIA ON CYBER SECURITY

Social media plays a vital role for hackers to break security. Because with time people participate in social media also increasing and companies should try to find out ways to protect personal data of the society by solving those issues of data and information leakage. In social sites personal data very easily can be leaked out.

In terms of Cyber Stalking, it's the key to harm a person on Social Networking. Criminals stalk the profiles of people on social media and based on post and activity they choose a person to take benefit of them.[8]

E.g. - If you are a well- earning or a rich person and you post on social media the car you buy or the hotels, restaurants, and clubs you visit and all other stuff that highlights your financial status and you don't apply privacy on sharing these things. It can harm you because you don't know which kind of person is watching those if you don't apply privacy on that. So, it is important to use privacy on sharing personal things on social media like your contacts and known-ones. Some people post quotes and posts like they are all alone which benefits a criminal. Because now he/she knows that you are Loner and Now he/she talks you very politely and through the screen, we cannot judge a person and through it is very easy for a person to share about his/her life because no-one is going to judge you in that state of mind people share some data which is private. [21] Due to this Social Scams originate. Criminals also build their profile like that he/she should have mutual friends together. So, you should confirm that with your friends.

7.1 Case Study

In 2013, at Hyderabad police arrested a youngster named Santosh Kumar assaulted a girl named Kiran from Bangalore. He created a fake Facebook profile of her. He also made threats calls and messages to the victim family. The complaint was reported by the victim's brother. [8]

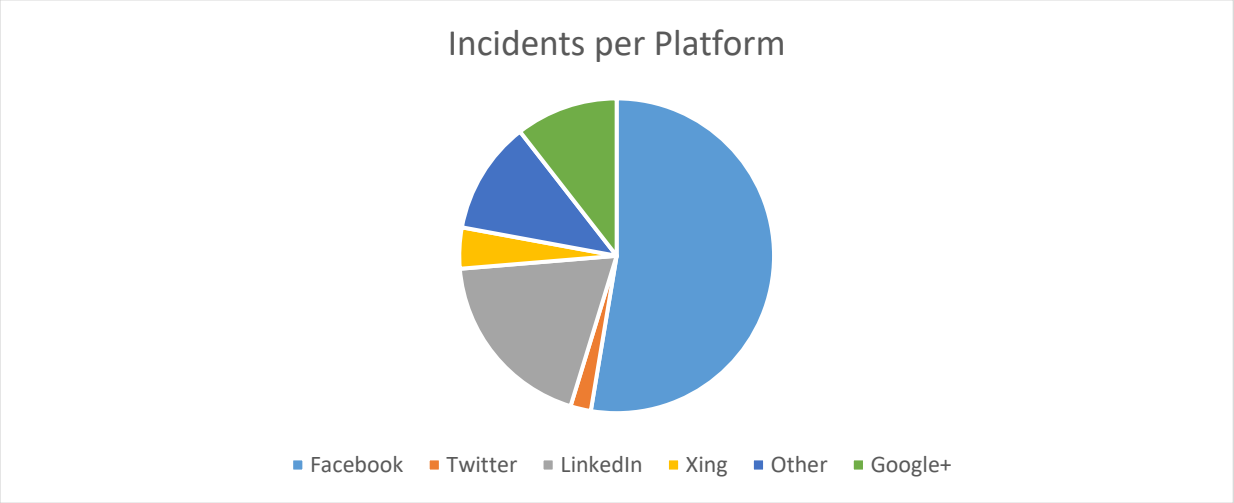

Fig. 7.1 Percentage of Scamming Threats Sites 2019[11]

8. NECESSITY OF CYBER SECURITY

Today data and information are the most valuable asset concerning any individual, private sector as well as government sector. Therefore the security of that data is very essential and important for an individual as well as for an industry too. By providing security to our devices we can protect ourselves from being hunted by cyber-attacks. The concerned points for the necessity of cyber security are [1]-

- Providing unauthorized access by CIA confidentiality, integrity, and availability.
- Security during online transactions regarding bank, shopping, payments, etc.
- Prevention from cyber-attacks and being prey in cyber-crime.
- It also increases the lifetime of the device.

9. CYBER CRIME

It is defined in its name itself that any kind of crime done with the help of a computer or internet that harms anyone is said to be a cyber-crime. They also include [1] –

- Trafficking in child pornography
- Stealing identities
- Violating privacy
- Money laundering
- Counterfeiting
- Hacking
- Cross-site scripting
- Cyber stalking
- Data diddling
- Cyber Bullying.

9.1 Case Study

9.1.1 Case-1

In 2019 a Face app has been launched that can change a person picture to old age to childhood and childhood to old age as well. The app has been in trend in a very short duration but the app recorded a lot of biometrics information about the people who used the app. The data of our biometrics is very valuable and somehow if it got leaked it can lead out to major problems.

9.1.2 Case-2

In India April 2014, Two under-graduate students Vivek Kumar and Anand Mishra who lives in Allahabad were arrested for online fraud they made a fake online to provide goods in Delhi and got hold to ATM pin of name Mahmood

and had 1.20 lakhs INR. These students get arrested and later they also confessed their crime. This case had been registered under IPC Act, Section 419, and 420 under IT Act, Section 66.

9.1.3 Case-3

There are thousands of cases that proofs that banking is a major attraction to hackers to exploit users. In 2019, Delhi a person named Rahul gets affected by it. Some anonymous hacker injected Trojan in his device and makes an online transaction to fake account of Rs.25, 000 (INR). He fired FIR for his loss. After 3 months of investigation police caught the culprit. [15]

It has been observed that only about 40% of cyber-crimes has been reported to the police stations. An individual needs to report any kind of cyber-crime or assault to happen with him/her. It can prevent a lot of other people from being prey of cybercrimes like this.

10. DOMAIN AREAS WHERE CYBER SECURITY CANNOT BE COMPROMISED

10.1 Defense

National Security is one of the major priority for a nation. By accessing defense satellites, terrorists can easily harm any nation by launching it for their benefits. It can affect millions of lives. So, each country/nation needs to ensure high cyber security to the area where the nation lack [25]. Terrorism is increasing with the increase in population. People discriminate against themselves based on religion, language, and colour. Cyber terrorism is a kind of attack against a nation that results in violence. It can be done by the brainwashing of people. Converting them into sleeper cells.

10.2 Hospital Data

All the data has been stored online these days. An intruder (hacker) can easily tamper the Personal records of the Patients or can affect its integrity. Like they can temper the reports of patients, their reason for coming to the Hospital. As we all know, there is a virus known as "CORONA" or "COVID-19" spreading across the world. [18] The virus is transferring enormously from one patient to another. In these cases, prior is to secure the data of a patient so that no further miss-happenings with the privacy of the patients. [14]

E.g.-Let's assume a hospital sends a patient's medical reports/ laboratory test reports or stores patient data in their database. An intruder can tamper it if security is not provided to them. Here to provide security to the data we can use encryption-decryption phenomena to secure our data.

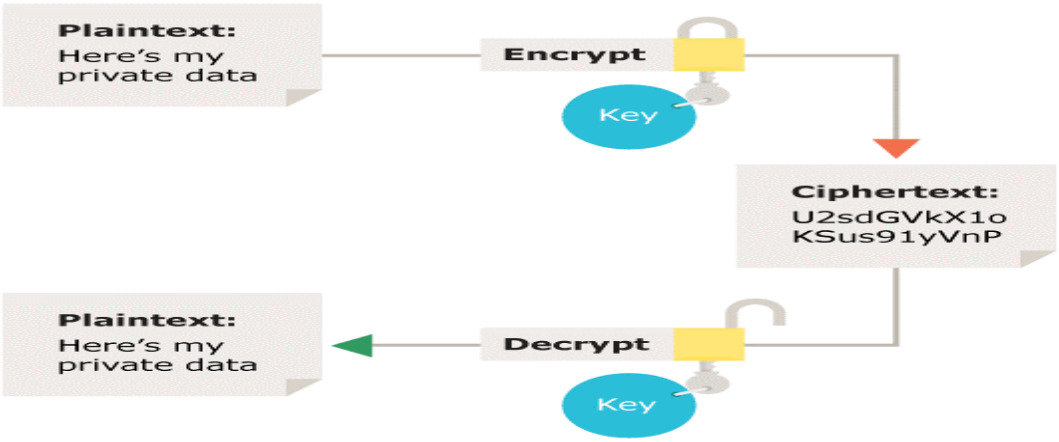

Fig. 10.1 Encryption Decryption Algorithm [13]

By encryption the data is converted into cipher text therefore the intruder cannot able to understand it or decrypt it without the key. In that way our data is being protected from them. Only those people can access the data that have the decryption key.

10.3 IT Ccompanies

There is no doubt how important cyber security is for IT companies. Their main objective is to keep the company data secure, if securing power of the company is weak it can easily be affected by the various cyber threats and the consequences of which could lead to a huge loss of Economy to them and their employees or may it can ruin the whole company.

10.4 Cloud Storage

It's 2020, the age of cloud storage and nowadays everyone is switching on the cloud to store their data because it provides a lot of benefits such as security, back up, Easy Sharing, Automation, etc. But still there are also cyber security threats in there.

10.5 Education Sector

In education today is a trend in online classes and the results of exams are uploaded on the internet. A lot of competitive exams are conducted online these days. So, it is important to ensure security to the same.

10.6 Banking

Now the whole banking system goes online most of the transactions has been done online these days' mainly big ones. So, in this area cyber-attacks are seen more often that's why this area requires more security.

FUTURE WORK AND CONCLUSION

This research paper highlights the importance of cyber security and the challenges faced for cyber security in the current era of the number of interconnected systems. [23] It also examines the internal infrastructure of cyber security and what is the threat that affects the CIA of a device and a user and ensure the CIA by taking proper measures and preventions. Further it describes the security of a mobile device, cyber ethics role on the internet. Cybercrime is also increasing as the technology increases and the paper shows us how cyber-crime affecting society and people too.

REFERENCES

[1] G. Nikhita Reddy, G.J. Ugander Reddy, 2016 “A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies” pp1-5.
[2] Jitendra Jain, Dr. Parashu Ram Pal (Professor, MCA Lakshmi Narayan College of Technology, Bhopal, M.P., India.), 2017 “A Recent Study over Cyber Security and its Elements” pp1-3.
[3] Atul M. Tonge, Suraj S. Kasture, and Surbhi R. Chaudhary, 2013 “Cyber Security: Challenges for society – Literature review” pp67-74.
[4] I. Duic, V. Cvrtila, T. Ivanjko (University of Applied Science Vern, Zagreb, Croatia), 2017“International Cyber Security Challenges” pp1525-1529.
[5] Brijesh Kumar Pandey, Alok Singh, Lovely Lakhani Balani(TIMSCDR), 2015 Mumbai "ETHICAL HACKING (Tools, Techniques and Approaches)" pp1-7.
[6] Mohammad Ghiasi, Moslem Dehghani, Taher Niknam, Abdullah Kavousi-Fard (Shiraz University of Technology, Shiraz, Iran. “Investigating Overall Structure of Cyber-attacks on Smart Grid control Systems to Improve Cyber Resilience in Power System”. pp1-6.
[7] Amit Wadhwa, Neeraj Arora "A Review on Cyber Crime: Major Threats and Solutions". pp1-6.
[8] Esther Ramdinmawii, Seema Ghisingh, Usha Sharma,2014, Don Bosco College of Engineering and Technology, Assam, India."A study of Cyber –Crime and Cyber Criminals: A Global Problem"pp1-9.
[9] Mirdul Sharma and Satvinder Kaur,2019 “Cyber Crimes Becoming Threat to Cyber Security” pp1-5.
[10] Aparna Srivastava,2017 “Analyzing Cyber Crime and Cyber Laws in India” pp1-3.
[11] htttp://fraudwatchinternational.com/ceo-fraud-a-quick-guide/
[12] http://cahare.sh-original-media.com/cyber-security-chart/
[13] https://blogs.dgplug.org/ritik5049/types-of-encryption
[14] Mohammad S Jalali,Jesica P Kaiser,2018 "Cyber Security in hospitals: A Systematic, Organizational Perspective"pp1-8.
[15] Dr. Manisha M More, Meenakshi P. Jadhav, Dr. K.M. Nalawade "Online Banking and Cyber Attacks: The Current Scenario". pp1-8.
[16] Susheel Chandra Bhatt, Durgesh Pant “Study of Indian Banks Websites for Cyber Crime Safety Mechanism”. pp1-4.
[17] Zoe M.King, Diane S. Henshel, Liberty Flora, Mariana G. Cains, Blaine Hoffman and Char Sample "Characterizing and Measuring Maliciousness for Cyber security Risk Assessment”pp1-5.
[18] Gianclaudio Malgieri, Data Protection and Research: A vital challenge in the Era of Covid-19 Pandemic, Computer Law & Security Review: The International Journal of Technology Law and Practice (2020). pp1-6.
[19] Zahid Maqbool, Palvi Aggarwal, V.S. Chandrasekhar Pammi and Varun Dutt "Cyber Security: Effects of Penalizing Defenders in Cyber-Security Games Via Experimentation and Computational Modeling” pp1-7.
[20] Lehto, M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. In N. Abouzakhar (Ed.), ECCWS 2015: Proceedings of the 14th European Conference on Cyber Warfare & security, University of Hertfordshire, Hatfield, UK, 2-3 July 2015 (pp. 179-188).
[21] Paul Benjamin Lowry, Jun Zhang, Chuang Wang, and Tailai Wu.” Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self Control, Rational Choice, and Social Learning” pp1-15.
[22] Michael Winterrose, Kevin Carter, Neal Wagner and W.W. Strelein "Adaptive Attacker Strategy Development Against Moving Target Cyber Defenses” pp1-8.

[23] Jessica Dawson and Robert Thomson "The Future Cyber security Workforce: Going Beyond Technical Skills for Successful Cyber Performance" pp1-5.
[24] P. Ramesh Babu, D. Lalitha Bhaskari, CH. Satyanarayana, 2011 "A Comprehensive Analysis of spoofing" pp1-7.
[25] Col. DImitrios Choupis, GRC Challenges and objectives for the National Cyber Security Strategy Beyond 2020" pp1-10.