MCS-215: Security and Cyber Laws

Dear learner, welcome to this course,

In the era of Information communication technology, it is essential to have in depth knowledge pertaining to Cyber security and laws governing cyberspace. After going through this course, the learners will be able to:

- Explain the security issues /breaches in cyberspace.
- Describe Cryptography Mechanisms.
- Discuss the concept of data security and management
- Explain the concept of security policy and security Audit
- Discuss various types of cybercrimes including Intellectual property issue in cyberspace
- Analyse the need and the present law governing / regulating cyberspace in India and in few selected countries.

This course consist of two Blocks, **Block-1** is titled Cyber Security Issues have 3 Units in which Unit-1 describe the Cyber security issues and challenges, Unit-2 deals with Cryptography Mechanisms and Unit-3 provide how the data can be secure and managed in Cyber space. **Block-2** of this course deals with cyber laws and provides an overview in Unit-4, how the Cyber space can regulated, Unit-6 comprehend various form of Cyber crime and the existing legal frame work in India. The concern of Intellectual property Rights issues emerging from Cyber space has been also discussed in the Unit-6. The unit also provides for regulatory frame work available in Indian and in International arena.

Course Expert Committee

1) Dr. V.V.Subrahmanyam, Director, SOCIS, IGNOU
2) Prof. S. Balasundaram, School of Computer and System Sciences, JNU, New Delhi
3) Prof. Sonajahria Minz, School of Computer and System Sciences, JNU, New Delhi
4) Dr. Aditi Sharan, School of Computer and System Sciences, JNU, New Delhi
5) Dr. Sanjay Kumar Dubey, Amity University, Noida Campus.
6) Dr. Rahul Johri, GGSIPU, New Delhi
7) Dr. Gurmeet Kaur, Assistant Professor, School of Law, IGNOU
8) Dr. Anand Gupta, Assistant Professor, School of Law, IGNOU
9) Dr. Shashi Bhushan , Associate Professor, SOCIS
10) Dr. P.V.Suresh, Associate Professor, SOCIS
11) Sh. Akshay Kumar, Associate Professor, SOCIS
12) Sh. M.P. Mishra, Assistant Professor, SOCIS
13) Dr. Sudhansh Sharma, Assistant Professor, SOCIS

Course Coordinators: **(1) Dr. Gurmeet Kaur, SOL, IGNOU**
(2) Mr Akshay Kumar, SOCIS, IGNOU

Course Preparation Team- Block-1

Unit Writers
Mr. Anand Raut (Unit-1)
Asstt. Professr, MNLU, Mumbai

Sh. Narayan Mahapatra (Unit-2)
IT Head, CCRYN, Ministry of Ayush

Ms. Kiron Prabhakar (Unit-3)
PAV Law Offices

Language & format Editor
Dr. Gurmeet Kaur, SOL, IGNOU

Content Editor
Ms. Kiron Prabhakar (Unit-1&2)
PAV Law Offices
Dr. Anupam Jha, Assoc. Prof.,
Faculty of Law, University of Delhi (Unit-3)

Course Preparation Team- Block-2

Unit Writers
Dr. Gurmeet Kaur, SOL, IGNOU (Unit-4&6)

Dr. Anand Gupta, SOL, IGNOU (Unit-5)

Language & format Editor
Dr. Gurmeet Kaur, SOL, IGNOU

Content Editor
Ms. Kiron Prabhakar
PAV Law Offices

Unit 1: CyberSecurityIssues and Challenges

Structure

1.0 INTRODUCTION

Information Technology is a dual edged sword. It is can be used for the betterment of mankind like in telecommunications, governance, public health, education, research, finance etc. but may also be used for disruptive purposes. Cyber security provides protection against use of information technology for disruptive purposes. This cyber security is nothing but technologies, processes, practices to protect computers, computer networks, and computer systems from cyber-attacks. In addition to technology there are certain laws which penalise commissions and omissions posing threat to cyber security.Remedies provided by laws include compensation, imprisonment, forfeiture, fine etc. Primary legislation regulating information technology is Information Technology Act 2000 and allied rules and regulations. The Information Technology Act 2000 defines and prescribes punishment for acts and omissions which poses threat to cyber security. The Act provides long arm jurisdiction meaning there by Courts in India have jurisdictions against the perpetrators of cyber offences not only residing in India but also in foreign countries. The Act also provides for the definition of cyber security under Section 2(nb) which states that cyber security is protection of information, devices, equipment, computer, computer resource, communication device as well as information stored from any use, un-authorized access, disclosure, disruption, modification and destruction(**IT act, sec2, https://www.indiacode.nic.in/).** Due to increasing cybercrimes, countries have become more aware of such exploitation and are taking necessary steps to curb exploitation by protecting their data through 'cyber security' from getting exploited.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- Explain the meaning and need of cyber security.
- Explain pros and cons of digital security
- Discuss ways in which cyberspace security is breached
- Explain technologies which can play significant role in providing cyber security
- Explain laws which aim at protecting cyberspace and prescribe penalty or punishment for those who pose threat to cyber security

1.2 DIGITAL SECURITY: PROS & CONS

Digital security is a broader term which encompasses within itself protection of online identity data assets Technology with the use of various tools like software, Web Services, biometrics, firewalls, proxies, vulnerability scanner, instant message or telephone encryption tools etc. Digital security provides protection against cyber-attacks unauthorised access, online malicious activities etc.

The 3 pillars of digital security are**(Mark Burnette, 2020, p.1**):

1. Confidentiality
2. Integrity
3. Availability

The basic essence of these principles is that the information which is private should be shared with the least amount of people to keep it more secure, the information provided should not be modified or corrupted and lastly, that the information provided should work effectively and efficiently at all times.

The OECD Recommendation and its companion documents were published in 2015 which provides guidance for all stakeholders on cyber security aspects. The Organization for Economic Cooperation and Development (OECD) helps in facilitating information, data and is progressing to eradicate poverty and inequality by bringing forefront solutions for the benefit of the world. The OECD Working Party on Security and Privacy in the Digital Economy (SPDE) develops public policy analysis and high-level recommendations to help governments and other stakeholders to ensure that digital security and privacy protection foster the development of the digital economy. (**OECD, 2015, p1)**

1.2.1 Digital Security: Pros

- It helps in protecting personal information stored in devices.
- Suspicious or unauthorized access to devices can be blocked through digital security and thus preventing possible harm.
- Security based on biometrics is capable of providing a higher degree of protection against attacks as it's difficult to steal biometric information.
- Digital security enables oneself to fearlessly communicate, transact, work etc. in online mode.
- Protects the computer from crashing or slowing down and thus protects business, transactions, communication etc. happening over computer, network or system

- Digital security thus may help in fostering the economy of the State as it cuts down on many costs.

1.2.2 Digital Security Cons

- Availing services or procuring tools for digital security can be a costly affair.
- Web services or tools may or may not be compatible with the device of the user.
- Digital security services or tools may be difficult to configure at times and needs to be updated regularly
- Services or tools may slow down functioning of user's device or at times may intervene even normal functioning of another programme

Please answer the following Check Your progress.

Check Your progress 1 *Spend 3 Min*

Write any three benefits of Digital Security?

1.3 SECURITY ISSUES /BREACHES IN CYBERSPACE

"Cyber Space" can be defined as a virtual space or to be more specific an electronic medium that is used to facilitate exchange of ideas via electronic means. The crimes which take place in the cyber space are termed as "cybercrimes".

A 'cyber incident' is defined under the section 2(e) of the CERT Rules as "any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public health or safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation".(**Ministry of Electronics and Information Technology Notification, 2018, p6**)

Threats to cyber security have been evolving from time to time and newer threats seem to emerge day by day. It's difficult to cover all of them however following are the most common security issues witnessed in cyberspace in recent past.

1. **Unauthorised access**– It is accessing computer, computer, network, system or device without permission from those who are authorized to access the same.

   Eg. Mr. Shyam spies on Ms. Rita and gets to know unlocking pattern set on her mobile device. Then Mr. Shyam without permission of Ms. Rita access pictures stored in her mobile device. This is an unauthorized access. Another example would be Mr. Shyam knows email address of Ms. Rita but not password. He tries different permutation and combination of passwords and finally gets access to all the emails

received by Ms. Rita. Unauthorized can be in the physical form too. Let's say Ms. Rita without permission from Ms. Shyam steals his pen drive and then accesses data stored in it. This acts also amounts to unauthorized access. Similarly stealing credit/debit card and then trying to use it for siphoning someone else's money involves element of unauthorized access.

2. **Distributed Denial of Service Attack** - It is aimed to adversely affect functioning of a website by sending multiple requests to a website which is beyond its control to handle. It's an attack on a machine or network resource to make it unavailable to intended users by flooding it with unnecessary traffic.(**GOsafeonline (2014**). Mr. AB creates a botnet herd which upon the command from control and command server sends huge amount of data to a server hosting a banks website resulting slowing down of the website. This is an example of denial-of-service attack on the bank.

3. **Malwares** - Malwares are software which are designed to harm network or device. It includes Botnets, Ransomwares, Trojan, Virus, Worms, Spywares etc. Botnets are collections of devices connected through the internet and infected with malware so the same may be controlled to carry out cyber-attacks. Ransomwares are malwares which encrypts files, data etc of the victim and then demands ransom from the victim to decrypt or permit access to files or data. Trojan is a malicious software which prima facie looks legitimate but is intended to steal, harm, damage device of victim. Term trojan has been picked from an ancient Greek story where a large structure resembling a horse was used to lead an attack against the city of Troy. Virus is a malicious programme which is designed to affect the functioning of a computer/device in which it is executed and capable of spreading from one computer to another. Virus is a malicious programme capable of self-replicating and spreading across networks. Spywares are malicious software which are installed in victims' devices without his knowledge to secretly spy and gather information of victims.

   Eg. One of the most infamous malware till date is ILOVEYOU malware spread in the year 2000. The mail prompted the victim to download 'LOVE-LETTER-FOR-YOU.TXT.vbs' attachment. The malware was in fact a worm and it overwrote system file and personal files of those who ended up downloading them.

4. **Social Engineering attacks** - These attacks harp upon psychological manipulation of victims and tricking the victim into revealing sensitive information. The victim is tricked to click on a malicious link or respond to fraudulent mail etc.

5. **Phishing** - It's an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity. Coining of term 'phishing' is inspired from term fishing as in fishing, bait is cast to fool fishes similarly deceiving message/mail/webpage is cast to fool innocent online user. Eg. Employee Ms. CD apparently receives a mail from Finance Officer of the Company in which she is working. The mail is in fact sent by an imposter who has disguised himself/herself as Finance officer.

6. **Crypto jacking** - It is unauthorised use of victims' device to secretly mine crypto currency. Crypto currency is a virtual currency with no central regulatory or issuing authority and secured through crypto currency. Crypto jacking affects the functioning

of devices as the same takes a toll on the device. For e.g Malwares use CPU's for mining crypto currency.

7. **Exploiting vulnerability**- Vulnerability is a flaw in the measures taken to secure a device. Such flaw is exploited by the attacker to gain access over the device or harm it.

8. **Cyber physical attacks** - These are cyber-attacks breaching the security and impacting the physical environment. This may include shutting down of cameras, lights etc. which are cyber controlled.

   E.g. Cyber attacker takes control over water pumps controlled by technology and causes destruction to property. Attacker taking control over cooling systems in nuclear reactor has the potential to inflict tremendous harm and pose threat to national security and safety.

9. **Internet of Things (IOT) attacks** - Embedded devices that are connected to a network and capable of transferring data are at the risk of being attacked through exploiting vulnerability and can be hacked.
   For e.g., Fax machines connected to internet may be exploited with their vulnerability and data can be stolen.

10. **Web Jacking** - Web jacking a term inspired from hijacking, means hijacking a website or its access and control is taken over by the attacker. This taking over is then misused for tricking the visitors of a website or deface the website.

11. **Drive by download** - A legitimate website is compromised and when the victim browses such a compromised website, the same installs malicious payload in the victim's device. This malicious payload can be in the form of ransomware.

    Some of the common security issues witnessed in cyberspace in recent past are as follows: (**Dr S.R. Myneni, p472-473**).

    1. **Internet time theft**: This involves usage by unapproved persons of the internet hours paid for by another person.

    2. **Key Loggers**: It is a software database or a program intended to covertly keep an eye on and log all keystrokes. The Key logger software scans computers, their processes, and data, the moment a person hits a key on the keyboard. This information is straightaway transmitted over to an external control.

    3. **Website defacement**: This is usually transmitted by the replacement of the homepage of a site by a system cracker that dislocated into a web server and modifies the hosted website creating one of its own. The attacker usually replaces the site matters with his own message or completely destroys the site's contents.

    4. **Pharming**: This takes place when the attacker redirects a user from an authentic and genuine site to a fake and deceitful site where their systems are infused with malware.

5. **Phreaking**: This refers to people who interfere with systems of telecommunication such as public networks.

6. **Email bombing**: This refers to forwarding a significant large number of emails to the victim resulting in the victim's email account or mail servers to not respond.

Check Your progress 2 *Spend 3 Min*

What is Phishing and whether it is challenge to digital security?

1.4 TECHNOLOGY'S ANSWERS TO CYBER SECURITY

1. **Unauthorised access** - Strong passwords, endpoint security, two factor authentications, physical security practices, monitoring user activity are few of the common practices employed for protection against unauthorized access.

2. **Distributed Denial of Service Attack** – Various infocom security tools are used to protect against DOS Attack like anti malware, firewall, spam filtering, switches and routers, Intrusion prevention systems, DDOS defence systems, content delivery network etc.**(GOsafeonline,2014)**

3. **Malwares** - a. Botnets - VPN, secured network architecture, traffic management tools etc. can help in detecting and preventing botnet attack. b. Ransomwares - Backing up data, disabling unnecessary ports or services such as RDP can help in preventing ransomware attack c. Trojan - robust firewall, anti-spywares, maintaining cyber hygiene are helpful against trojans d. Virus - Malware removal software, automatic scans can reduce the risk of virus attacks, e. Worms - Internet connection firewall, network intrusion detection software, use of Domain Message Authentication Reporting (DMARC), Domain Name System Security Extension (DNSSEC) can be helpful. f.

4. **Spywares** - Anti spywares, sandbox protection, ad pop up blockers can play significant role in averting spywares.

5. **Social Engineering attacks** – network traffic analysis, firewalls, updated software, spam protection guards, updated blacklists(**Chizari, Hassan &Zulkurnain, et al (2015**) can aid in preventing social engineering attacks. However, it is considered that the most efficient way to tackle social engineering attacks are awareness about such attacks. Social engineering attacks thrive on people's ignorance and hence awareness is the key to fight against such attacks.

6. **Phishing** - SPAM filters, web filters, patching, use of SSL certificate to secure traffic are a few technologies which may assist in combating Phishing attacks.

7. **Cryptojacking-** anti crypto mining extensions, endpoint protection, web filtering tools, network monitoring solutions etc are helpful in preventing crypto jacking.(**Micheal Nadeau,2021),**

8. **Exploiting vulnerability** – Patching operating systems, enabling SMB signing, network segmentation which limits access to systems etc. may reduce the chances of exploitation of vulnerability.

9. **Cyber physical attacks**- Adequate control on physical access, cyber nodes, enabling remote access only when necessary, two factor authentications etc. are few of the practices which have turned out beneficial in combating cyber physical attacks.

10. **IOT attacks** - Firmware updates with cryptographic signatures, proper identity management, hardened toolchains, libraries and framework, etc may be used for protection against IOT attacks.

11. **Web Jacking** - Web Server firewalls, X frames options etc may be used to prevent web jacking.

12. **Drive by download** - Updating website components, web security software etc. can provide protection against drive-by download.

1.4.1 Cyber Security Intrusion Detection

Intrusion detection systems monitor traffic and generate alerts in the case of suspicious activity tending to harm the cyber security. However, some intrusion detection systems are capable of even prevention of cyber threats. Such intrusion systems may be network, host, hybrid, application, protocol based and method of detection may be signature based or anomaly based. Signature based intrusion detection system detects intrusions based on patterns or already known malicious instruction sequence. Anomaly based systems rely on trustful activity model with the use of machine learning and anything dissimilar from the model is alerted as suspicious. With the rise of IOT based environment use of such intrusion detection systems have grown multi fold.(**Elrawy, M., Awad, A. & Hamed, H**, **2018**) Intrusion detection systems can help in ensuring IT related regulatory compliance, maintain security standards, and raises alarms against malwares like spywares, keyloggers, unauthorized clients, unintentional accidental leakage etc., and measure the cyber-attacks in number and forms/types, increase efficacy. However, such detection systems are susceptible to few flaws like it has been witnessed that such systems often raise false alarms, unable to avid encrypted packets, they need to be continually updated and generally should be looked after by an expert engineer.

Strong Passwords, Firewalls, Encryption, Digital Signature, Clipper Chip, Routers/Gateways, Free software programs like security administrator tool, COPS, Omni Guard and Net probe which can identify any obstacle in the security mechanism and can be adopted to be safe at all times.

Check Your Progress 3 *Spend 3 Min*

Name any three cyber security software to fight against cyber-attacks?

1.5 CYBER SECURITY AND THE LAW

Cyber Law has played an instrumental role in regulating security issues and breaches in cyber space. Cyber law consists of Acts, Rules, Regulations, Notifications etc. passed by the Government of India. Information Technology Act 2000 is primary legislation governing cyber security in India. Besides, Government has also established Computer Emergency Response Team, Cyber and Information Security Division of Ministry of Home affairs, National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Coordination Centre, National Cyber Security Coordinator, Defence Cyber Agency etc to ensure cyber security. Cyber security law is concerned with integrity, confidentiality, availability of public private information systems and seeks to protect individual rights like privacy, economic interests and national security.(**Jeff Kosseff, 2018**)

1. **Unauthorised access** - Unauthorised access is prohibited by law. As per Section 43 (a) of Information Technology Act 2000 (hereinafter IT Act 2000) makes any person liable for compensation if he is without permission of owner or any other person in charge of computer, computer system, computer network access or secures access. If the aforesaid act is done fraudulently or dishonestly then the person shall be liable for punishment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

2. **Distributed Denial of Service Attack** - As it is aimed to affect functioning of a website the act of carrying out Distributed Denial of Service attack shall disrupt computer network or computer system. It may also cause denial of access to persons who are authorised to access the said website. Aforesaid acts are prohibited by Section 43 (e) and (f) of IT Act 2000 respectively. Also, if denial of access attack is carried out with intent to threaten the unity, integrity, security or sovereignty of India or to striketerror in the people or any section of the people then the same shall be punishable under Section 66 (f) of IT Act 2000 with imprisonment for a term which may extend to imprisonment for life.

3. **Malwares** - Malwares like Botnets, Ransomwares, Trojan, Virus, Worms, Spywares etc. can be categorized as computer contaminants. Malwares are capable of modify, destroy, transmit data of programme residing in computer, computer network or computer system or usurp normal operation of the same, hence it is a contaminant as per Section 43 Explanation 1 (a). Malwares are capable of destruction, damage or adversely affect performance of a computer resource or capable of attaching itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource and hence includes computer virus as per Section 43 Explanation 1 (b) of IT Act 2000. Introduction of the malware leads to cyber contravention under Section 43(c)of IT Act 2000 and make the person who introduces it liable for damages by way of compensation. Similarly, if the introduction of computer contaminant or virus results in to destruction, deletion or alteration of information residing in computer resource or diminishes its value or utility or affects injuriously or steals, conceals, destroys or alters any computer source code used for computer resource with an intention to cause damage then it shall lead to

damages by way of contravention under section 43 (i) and (j)of IT Act 2000. If any of the aforesaid activities are carried out fraudulently or dishonestly then Section 66 of IT Act 2000 prescribes punishment of imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

4. **Social Engineering attacks** - These attacks harp upon psychological manipulation of victims and tricking the victim into revealing sensitive information. The victim is tricked to click on a malicious link or respond to fraudulent mail etc. Phishing - Its an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity. Coining of term Phishing is inspired from term fishing as in fishing, bait is cast to fool fishes similarly deceiving message/mail/webpage is cast to fool innocent.
As these attacks are carried out through impersonation, they are punishable under Section 415 of Indian Penal Code 1860. Also use of communication device or computer resource to cheat by personation is made punishable under Section 66D of IT Act 2000 is punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. Social engineering attacks are carried out to steal electronic signature, password or any other unique identification feature and hence the same is punishable under section 66C for identity theft which is punishable for a term which imprisonment of either description for a term which may extend to three years and shallalso be liable to fine which may extend to rupees one lakh.

5. **Cryptojacking** - It is unauthorised use of victims' devices to secretly mine cryptocurrency. Cryptojacking affects the functioning of devices as the same takes a toll on the device. Cryptocurrency is a virtual currency with no central regulatory or issuing authority and secured through cryptocurrency. Section 43 (a) and Section 66 of Information Technology Act 2000 prescribes compensation and imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both respectively.
6. **Exploiting vulnerability**- Vulnerability is a flaw in the measures taken to secure a device. Such flaw is exploited by the attacker to gain access over the device or harm it. Vulnerability is exploited and unauthorized access is secured. This is punishable under Section 43 (a) and Section 66 of IT Act 2000.

7. **Cyber physical attacks -** These are cyber-attacks breaching the security and impacting the physical environment. This may include shutting down of cameras, lights etc which are cyber controlled. Section 43 (d) and 66 of Information Technology Act 2000 prescribes penalty for causing damage and prescribes imprisonment if damage is caused with dishonest or fraudulent intention.

8. **IOT attacks** - Embedded devices that are connected to a network and capable of transferring data are at the risk of being attacked through exploiting vulnerability and can be hacked. Section 43 (a) of IT Act 2000 prescribes penalty for unsecured access and punishment under Section 66 of IT Act 2000.

9. **Web Jacking** - Webjacking a term inspired from hijacking, means when a website is hijacked or its access and control is taken over by the attacker. This is then misused for tricking the visitors of a website or defacement of a website etc. Section 43 (a) provides compensation for acts of unsecured access, Section 43 (d) and (e) penalises for causing

damage and disruption to computer network, computer system like what happen in defacement of website. Section 65 and Section 66 prescribes imprisonment and fine for unauthorised access and knowingly or intentionally conceal destroy or alter computer source code which generally happens during defacement of website.

10. **Drive by download** - A legitimate website is compromised and when the victim browses such a compromised website, the same installs malicious payload in the victim's device. Section 43 (c) prescribes compensation for introducing computer contaminant or virus and Section 65 of IT Act 2000 prescribes punishment for altering computer source code which may happen during drive by download attack. Besides, Information Technology Act 2000, Indian Penal Code 1860 is applicable to cyber offences, Trademarks law and Copyright law protects violation of Intellectual property in the form of domain names and software, Evidence law is helpful in prescribing the manner in which electronic evidence is admitted in the courts of law. There have been number of cases like altering of source code(Syed Asifuddin and Ors, 2005)Phishing,(NASSCOM case, 2005)data theft(Gagan Harsh Sharma case, 2019), hacking(M/S.Sundaramcase, 2011)etc. where courts of law have punished offenders guilty of breaching cyber security.

Selected Case Laws

1. In Pune Citibank MphasiS Call Center Fraud(**Malini Bhupta,2005),**employees of a Company cheated US customers of Citibank. The fraud involved securing unauthorized access to computer system which was punishable under Section 43 and 66 of Information Technology Act 2000.
2. In Syed Asifuddin and Ors. v. The State of Andhra Pradesh,2005, It was alleged that employees of a company manipulated electronic 32-bit number (ESN) programmed into Samsung N191 and LG-2030 cell phone instrument. This amounted to alteration of computer source code and the act was punishable under Section 65 of Information Technology Act 2000.
3. 26/11 Terror attack investigation revealed that terrorists hacked systems to access data with computer systems of hotels which were under attack. The attack squarely fell under Section 66F of Information Technology Act 2000**(Ilardi, Gaetano,2009)**
4. Abhinav Gupta v. State of Haryana, 2008, highlights that Stealing and sharing of confidential/copyright material falls within the ambit of Section 66 of IT Act 2000 and hence punishable.

1.6 SUMMARY

Challenges to cyber security exists in the form of unauthorized access, exploiting vulnerability, cyber physical attacks, IOT attacks, Web jacking, drive by download, crypto jacking, social engineering attack, malwares, denial of service attacks etc. These may be prevented with the help of technologies, practices and remaining vigilant. Few of the most common technologies or practices are updated firewalls, strong passwords, patching operating systems, two factor authentications, etc. which can help in preventing cyber security attacks. Law also acts as a deterrent factor for those who attack cyber security. Law prescribes punishment in the form of fine, imprisonment etc. for cyber law violations. Cyber

security attacks may also cause intellectual property violations and hence attract law regulating the same. An information technology law empowers enforcement agencies with investigative powers and recognizes electronic evidence admissible in the courts of law. However, threat to cyber security in the form of cyber-attack can be carried out anywhere in the World and hence for enforcement of cyber security law and bring culprits to justice it's necessary that all the States come together and collectively fight against those who pose threat to cyber security.

1.7 Solution and Answer

Check Your Progress

1 Benefits of Digital Security are:-
   a. Protection of Data
   b. Prevent unauthorized access
   c. Prevent cyber attack
   d. Builds trust in the integrity of online communication or transaction.

2 Phishing is an activity by which the victim is deceived to reveal sensitive information like username, passwords, credit/debit card details etc by disguising oneself as a trustworthy entity.Yes, it is threat to digital security.

3 Firewall, Firmware, Network intrusion detection software etc.

1.8 REFERENCES AND FURTHER READINGS

- Abhinav Gupta v. State of Haryana (2008 Cr LJ 4536)
- Andrew Murray(2013). *Information Technology Law: The Law and Society*. 2nd ed: Oxford University Press.UK
- Chizari, Hassan &Zulkurnain, Ahmad &Hamidy, Ahmad & Husain, Affandi. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science.* 1. 188-198.
- Dr S.R. Myneni. *Information Technology Laws*. First Edition.p497-519
- Elrawy, M., Awad, A. & Hamed, H (2018). Intrusion detection systems for IoT-based smart environments: a survey. *J Cloud Comp 7, 21. Retrieved from* https://doi.org/10.1186/s13677-018-0123-6.
- Gagan Harsh Sharma v. The State of Maharashtra 2019 CriLJ 1398
- GOsafeonline (2014).Denial of Service.Singpore Government Website Agency.Retrievdon 12/09/2020 from https://www.csa.gov.sg.
- Ilardi, Gaetano. (2009). The 9/11 Attacks—A Study of Al Qaeda's Use of Intelligence and Counterintelligence. *Studies in Conflict & Terrorism* - STUD CONFL TERROR. 32. 171-187. 10.1080/10576100802670803.
- Information Technology Act, 2000. Retrieved from https://www.indiacode.nic.in/.
- Jeff Kosseff (2018). Defining Cyber security Law.*103 Iowa L. Rev. 985*

- M/S.SundaramB.N.P.ParibasHome v. State of Tamil Nadu W.P.Nos.2513 of 2011.
- Malini Bhupta(2005). Pune call centre fraud rattles India's booming BPO sector, raises questions on security. Retrieved from https://www.indiatoday.in/magazine/economy/story/20050502
- Mark Burnette (2020). Three Tenets of Information Security. Retrieved from https://www.lbmc.com/blog/three-tenets-of-information-security/
- Micheal Nadeau (2021). 'What is crypto jacking? How to prevent detects and recovers from it'. Retrieved from https://www.csoonline.com/.
- Ministry of Electronics and Information Technology Notification (2018). Retrieved https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf
- NASSCOM v. Ajay Sood 119 (2005) DLT 596
- OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en
- Paul Todd (2015). *E-Commerce Law*. Taylor and Francis Publications.
- Sharma Vakul (2019). *Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce*. 6th Edition, LexisNexis, Haryana
- Singh Talwant, (2011). *Cyber Law & Information Technology*. New Delhi, India.
- Singh Yatinder Justice (2016). Cyber Law. 6th ed. Universal Law Publishing Co.India
- Steve Hedley and Tanya Aplin (Ed.) (2008). *Blackstone's Statutes on IT and e-commerce* 4th edition: Oxford.
- Syed Asifuddin and Ors. v The State of Andhra Pradesh And Anr. 2005 Cri LJ 4314.

UNIT-2 CRYPTOGRAPHY MECHANISMS

Structure

2.0 INTRODUCTION

One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and messages in transit and in storage. Cryptography has a long and colorful history. Historically, four groups of people have used and contributed to the art of Cryptography, the military, the diplomatic corps, diarists, and lovers. The military has had the most sensitive role and has shaped the field.

At present, information and data security plays a vital role in the security of the country, the security of the corporate sector and also of every individual, working for personal benefit.

2.1 OBJECTIVES

At the end of this unit, you will able to:

- discuss what is conventional cryptography and types of ciphers;
- explain the meaning of encryptions ;

- describe Algorithms used in Cryptology;
- discuss encryption schemes, their merits and demerits;
- explain the meaning and use of Electronic Signature;
- discuss cryptographic hash functions and cryptographic protocols and mechanism;
- describe methodology for ensuring the secure distribution of keys for cryptographic purposes; and
- explain the concept of trusted third parties and public key certificates.

2.2 INTRODUCTION to CRYPTOGRAPHY

The message or data to be encrypted, also known as the plaintext, is transformed by a function that is parameterized by a KEY. The output of the encryption process, known as the cipher text, is then transmitted through the insecure communication channel. The art of breaking ciphers is called cryptanalysis. The art of devising ciphers (cryptography) and breaking them (cryptanalysis) is collectively known as cryptology.

Mathematically, C = Ek (P) meaning that the encryption of the plaintext P using key K gives the cipher text C. Similarly, P = Dk(C) implies the decryption of C to get the plaintext again. It then follows that Dk (Ek (P)) = P.

Types of Ciphers

Conventionally, there are two types of ciphers. They are the following:

Substitution Ciphers: Another letter or group of letters to disguise it replaces each letter or group of letters. One of the oldest known ciphers is the Caesar Cipher**,** attributed to Julius Caesar. For example, using this cipher, attack becomes DWWDFN. Here plaintext is in lowercase and cipher text in uppercase letters. A slight generalisation of the Caesar cipher allows the cipher text alphabet to be shifted by k letters, instead of always 3.In this case k becomes a key to the general method of circularly shifted alphabets. Example in Fig. 1 shows:

JULIUSCAESAR Plaintext

EFGEFGEFGEFG Key EFG repeated

10 21 12 09 21 19 03 01 05 19 01 18 Plaintext, numeric

05 06 07 05 06 07 05 06 07 05 06 07 Key EFG, numeric

15 19 11 12 19 20 06 07 02 22 07 21 Cipher text (Plain XOR key)

Figure 1

A FUNCTION BASED SUBSTITUTION CIPHER

A substitution cipher can be made unbreakable by using a long no repeating key. Such a key is called one-time pad. A one-time pad may be formed by using words from a book starting from specific place known to both the sender and receiver. For example, starting with this sentence and using XOR on ASCII encoding of the letters of the plaintext and of the key. The encryption would proceed as given in Fig. 2.The textual equivalent of the cipher text is not given because it contains nonprintable ASCII characters. The message can be deciphered by reversing the process. XO Ring each letter of the cipher text with the ASCII representation of the key produces the ASCII encoding of a letter of the plaintext.

JULIUSCAESAR Plaintext

FOREXAMPLEST key-starting sentence (one-time pad)

74 85 76 73 85 83 67 65 69 83 65 82 Plaintext, ASCII

70 79 82 69 88 65 77 80 76 69 83 84 Key ASCII

12 26 30 12 13 18 14 17 09 22 18 06 Cipher text = Plain XOR key

Figure 2

A ONE-TIME PAD

One-time pad ciphers are unbreakable because they give no information to the cryptanalyst. The primary difficulty with one-time pad is that the key must be as long as the message itself, so key distribution becomes a problem, since a different pad must be used for each communication.

Transposition Ciphers: It operates by reordering the plaintext symbols, whereas substitution ciphers preserve the order of the plaintext symbols but try to disguise them. An example of it Columnar transposition is described below:

C O N S U L T Keyword

1 4 3 5 7 2 6 Column numbers

E N C R Y P T Plaintext:

I ONISP E ENCRYPTIONSPERFORMEDBYWRITINGTHEPLAINTEXT R FORMED
B YWR ITI

N G T H E P L cipher text:

AINTE X TEIRBNAPPETPXCNOWTNNOFYGIRIRRHTTEDILTYSMIEE FIGURE for Transposition Cipher.

The other types of ciphers which are present are as follows: (The Economic Times, 2021, p.1)

1. **Polyalphabetic substitution cipher**: In this cipher, a blended alphabet is utilized to encrypt the plaintext, but at random points it would convert to a special uncommon mixed alphabet which denotes the alteration with an uppercase letter in the Ciphertext.

2. **Transposition Cipher**: This cipher is also known as Rail Fence Cipher and is a permutation of the plaintext.

3. **Permutation Cipher**: The locations assumed by plaintext are moved to a uniform system in this cipher so that the ciphertext amounts to a permutation of the plaintext.

4. **Private-key Cryptography**: In this cipher, even the attacker is mindful of the plaintext and corresponding ciphertext. The sender and receiver must have a pre-shared key. The shared key is kept undisclosed from all other parties and is used for encryption as well as decryption. DES and AES algorithms are examples of this type of cipher. This cryptography is also known as "symmetric key algorithm".

5. **Public-key Cryptography**: In this cipher, two different keys - public key and private key - are used for encryption and decryption. The sender uses the public key to carry out encryption, whereas the receiver is kept in the dark about the private key. This is also known as asymmetric key algorithm.

2.2.1 Functions of Cryptography

Base cryptographic functions provide the most flexible means of developing cryptography applications. All communication with a cryptographic service provider (CSP) occurs through these functions. A CSP is an independent module that performs all cryptographic operations. At least, one CSP is needed with each application that uses cryptographic functions. A single application can occasionally use more than one CSP. Base cryptographic functions are in the following broad group

Service provider function
Key generation and exchange function
Object encoding and decoding functions
Data Encryption and decryption functions
Hash and Digital functions

The five key functions of cryptography are: (Gary C. Kessler, 2021, p.1)

1. **Privacy/Confidentiality:** Making sure that no one can persuse the message except the intended receiver.

2. **Authentication:** The process of showing and establishing one's identity.

3. **Integrity:** Assuring the receiver that the received message has not been distorted in any manner from the initial.

4. **Non-repudiation:** A process or a way to prove that the sender really sent this message.
5. **Key exchange:** The approach by which crypto keys are shared between sender and receiver.

Check your progress 1 Spend 3 Min.

Fill in the blanks:

i) The output of the encryption process is known as _____.

ii) Substitution and _____ are two types of Ciphers.

2.3 STEGANOGRAPHY

It is one of the techniques of hiding secret data within a non-secret, ordinary file or manages to avoid being deleted. It will be decoded at the station. In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as JPEG image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying, the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has noise patterns of regular, unencrypted data.

It can be divided into following five types:

- Text Steganography
- Image Steganography
- Video Steganography
- Audio Steganography
- Network Steganography

The benefit of this method is that the data is extra and twice as safe i.e., that first that it is out of sight and the second is that it is encrypted. Because of this process, it becomes challenging for the person to first locate or trace the data and then encrypt it.

Some of the well known uses of stego around the world include:
Head of the messenger was shaved and a tattoo was done on the head and after the hair grew back, the messenger was sent and the recipient again shaved the hair to read the tatooed message, U.S. Marine Corps Navaho code talkers of WWII, Disappearing ink and microdots, Osama bin Laden's pre-recorded videos that are re-played on TV stations around the world contain hidden messages, September 11 attacks in New York City, Washington, D.C. (Gary C. Kessler, 2001, p.1)

2.4 ENCRYPTION AND DECRYPTION

Encryption is one common method of protecting information transmitted over unreliable links. In practice, the following is the mechanism of encryption:

A) The information (text) is encrypted (encoded) from its initial readable form (called clear text), to an internal form (called cipher text). This internal text form, although readable, does not make any sense.

B) The cipher text can be stored in a readable file, or transmitted over unprotected channels.

C) The receiver must decrypt (decode) it back into clear text to understand the meaning of the cipher text.

Since it is likely that people may become involved with negative aspects of computing, care has to be taken to see that encryption algorithms are free from statistical and mathematical weakness and that they are not feasible to break computationally so that cracking becomes prohibitively time-consuming. At the other end, the computational complexity of encryption and decryption should be reasonable because they represent processing overhead that increases communication delays.

2.5 ENCRYPTION SCHEME: PUBLIC KEY AND PRIVATE KEY DISTRIBUTION

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both. This section highlights a number of these and summarizes features pointed out in previous sections.

Advantages of symmetric-key cryptography

1. Symmetric-key ciphers can be designed to have high rates of data throughout. Some hardware implementations achieve of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range. Keys for symmetric-key ciphers are relatively short.

2) Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators, hash functions and computationally efficient digital signature schemes, to name just a few.

3) Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyse, but are weak on their own weak, can be used to construct strong product ciphers.

4) Symmetric-key encryption is perceived to have an extensive history, although it must be acknowledged that, notwithstanding the invention of rotor machines earlier, much of the knowledge in this area has been acquired subsequent to the invention of the digital computer, and in particular, the design of the Data Encryption Standard in the early 1970s.

ii) Disadvantages of symmetric-key cryptography

1) In a two-party communication, the key must remain secret at both ends.

2) In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP.

3) In a two-party communication between entities μ and ¶, sound cryptographic practice dictates that the key be changed frequently and perhaps for each communication session.

4) Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP.

iii) Advantages of public-key cryptography

1) Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).

2) The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner, as opposed to in real time.

3) Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).

4) Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

5) In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

iv) Disadvantages of public-key encryption

1) Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best-known symmetric-key schemes.

2) Key sizes are typically much larger than those required for symmetric-key encryption and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.

3) No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.

4) Public-key cryptography does not have as extensive a history as symmetric-key encryption, being discovered only in the mid 1970s.

Summary of comparison

Symmetric-key and public-key encryptions have a number of complementary advantages.

Current cryptographic systems exploit the strengths of each. Public-key encryption techniques may be used to establish a key for a symmetric-key system being used by communicating entities and in this scenario, we can take advantage of the long-term nature of the public/private keys of the public-key scheme and the performance efficiencies of the symmetric-key scheme. Since data encryption is frequently the most time-consuming part of the encryption process, the public-key scheme for key establishment is a small fraction of the total encryption process.

To date, the computational performance of public-key encryption is inferior to that of symmetric-key encryption. There is, however, no proof that this must be the case. The important points in practice are:

1. Public-key cryptography facilitates efficient signatures (particularly non-repudiation) and key management; and

2. Symmetric-key cryptography is efficient for encryption and some data integrity applications.

Please answer the following Self Assessment Question.

Check your progress 2 **Spend 3 Min.**

What are the basic advantages of Asymmetric Key?

.....

2.6 COMMONLY USED CRYPTO ALGORITHMS

The Secret-Key Algorithm: A system where one secret key shared is called Symmetric or secret key cryptography. This approach is known as Caesar's Cipher and usually functions in the alphabet substitution technique. This is a very simple technique and in today's world encryption systems aren't as straightforward as one thinks.

2.6.1 Data Encryption Standard (DES):

It was originally developed by IBM and was adopted as an NBS Standard in 1977 to shield susceptible data, unarranged government data. It is no longer secure in its original form (Wayner, 1995), but in modified form it is still useful. DES is a symmetric cryptosystem, so the cipher text is decrypted using the same key. It operates on 64-bit (8 byte) blocks of input at a time. The algorithm, which is parameterized by a 56-bit key, has 19 distinct stages. The first stage is a key independent transposition on the 64-bit plaintext. The last stage is the exact inverse of this transposition. The stage prior to the last one exchanges the leftmost 32 bits with the rightmost 32 bits. The remaining 16 stages are functionally identical but are parameterized by different functions of the key.

The steps of the DES encryption algorithm operating on 64-bit block are:

L_0R_0 = t(input)

Repeat for n = 1 to 16

Ln = Rn□1

Rn = Ln□1 + f(Rn□1,Kn)

Output = t $^{□1}$ (L16r16)

Obviously, DES is a complex algorithm. But critics say that its key is too short, which makes it susceptible to brute-force attack. In 1977, two standford Cryptography researchers, Diffie and Hellman designed a machine to break DES and estimated it could be built for 20 Million dollars. Given a small piece of plaintext and matched cipher text, this machine could find the key by exhaustive search of the entry key space in under 1 day. Nowadays such a machine would cost perhaps 1 million dollars. A detailed design for a machine that can break DES by exhaustive search in about four hours is presented in (Wiener, 1994).

Another calculation says that software encryption is 1000 times slower than hardware encryption and that, a high-end home computer can still do about 3, 50, 000 encryption/sec in software and is probably idle 2 million second/month. This idle time could be put to use breaking DES. Probably the most innovative idea for breaking DES is the CHINESE LOTTERY (Quisquater and Girault, 1990). With this, every radio and television has to be equipped with a cheap DES chip capable of performing 1 million encryption /sec in hardware.

As DES was deciphered by the researchers as mentioned above, it was replaced by AES encryption algorithm. The greatest drawback is low encryption length and now TLS 1.2 is used. **(Jay Thakkar, 2020, p.1)**

Public Key Algorithms: A cryptosystem where two different keys are used for encryption and decryption is called Asymmetric or Public key System. The key distribution is the most important thing whatever may be the cryptosystem. If somehow the key is stolen, the total system would be worthless. The primary advantage of public key cryptography is increased security. The secret keys don't have to be transmitted or revealed to anyone. Another advantage of this system is that public key and the secret key can both be used for encoding as well as decoding. Their functions are interchangeable.

2.6.2 RSA Algorithm:

These are the initials of three discoverers (Rivest, Shamir, and Adleman) at M.I.T. They all produced this algorithm, which is totally based on modular mathematics of Number theory. It is an asymmetric cryptography algorithm because it uses two different keys for encoding and decoding.

One of the properties of modular arithmetic is the possibility of computing multiplicative inverses. That is, given an integer e in the range of [0, n□1], it is sometimes possible to find a unique integer d in the range [0, n□1] such that

ed mod n = 1

For example, 3 and 7 are multiplicative inverses modulo 20, because 21 mod 20 =

1. It can be shown that integer e [0.n□1] has a unique multiplicative inverse mod n when e and n are relatively prime, that is when gcd (e, n) = 1.(gcd denotes the greatest common divisor). The no. of positive integers that are relatively prime to n is a function denoted as @n. For n = pq and p and q are prime, it can be shown that

@n = (p□1)(q□1)

For number P set of [0, n□1] it can be shown that the equation

$C = p^e \bmod n$ (First) is an inverse of

$P = C^d \bmod n$ (Second)

If ed mod @(n) = 1 where @n = (p□1)(q□1)

First equation is used for encryption by several public keys algorithms with e and n as the key. Decryption is performed using second equation with d and n as keys.
Since the key (e, n) is public, only the number d in the decryption pair (d, n) is private.

This above idea is used in case of RSA also. The determination of n, d and e is prescribed in the following way:

Choose two large primes, p and q, each greater than 10^{100} Calculate n= pq and @n = (p□1)(q□1)

Assume a number d to be a large, random integer that is relatively prime to @n that is such that ed mod @(n) = 1

Calculate e such that ed mod @(n) = 1

These parameters may be used to encipher plaintext P where 0 less that equal to less than n. If the plaintext is longer, it must be broken into strings smaller than n. Cipher text is obtained as $C = p^e \bmod$

n. C may be then decrypted as $P = c^d \bmod n$. Steps of algorithm ensures that encryption and decryption are inverses of each other.

Yet breaking of RSA is not reported yet wide use of it has been tremendous increased. A cryptanalyst would presumably use factoring to derive d from n and e, which are publicly known.

Hybrid Encryption is the best of both symmetric and asymmetric encryption and the same is creating tough encryption techniques. But, both of them come with both pros and cons, symmetric encryption method is fast for large data encryption but falls short of identity verification. The assymetric encryption method is quite opposite, it is slow but have public and private key pair which is a must when it comes to cyber safety.
Now, in the present times, both identity verification and speed is a must and that is how the process of hybrid encryption came into existence. **(Jay Thakkar, 2020, p.1)**

Check your progress 3 Spend 3 Min.

Why is RSA algorithm more widely used than DES?
.....
.....

.....

2.7 ELECTRONIC SIGNATURE

People authenticate other people by recognising their faces, voices and handwriting. Signatures on letterhead paper handle proof of signing raised seals and so on. Handwriting, paper, and ink experts can usually detect tampering. But none of these options are available electronically. That's why the concept of Digital signature came into existence to authenticate electronic documents.

A Digital Signature is a technique by which it is possible to secure electronic information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called Authentication.

The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. For a computerised message system to replace the physical transport of paper and ink documents handwritten signatures have to be replaced by Digital Signatures. Basically what is needed, is a system by which one party can send a "signed" message to another party in such a way that

A) The receiver can verify the claimed identity of the sender.

B) The sender cannot repudiate the contents of the message.

C) The receiver cannot possibly have concocted the message himself/ herself.

A digital signature is only a technique that can be used for different authentication purposes. For an E-record, it comes functionally very close to the traditional hand-written signatures. The user himself/ herself can generate key pair by using specific crypto software. Now Microsoft IE and Netscape, allow the user to create his/ her own key pair.

Here, the most important thing is how can the user be sure that public keys belong to his/ her partner only? In this case, a third party (TTP) will guarantee the relationship between the identity and the public keys. The TTP are popularly called Certified Authorities (CAs).

Digital Certificate: These certificates are provided by CAs to authenticate that a particular site is globally secured. There are so many reputed CAs all over the world. Some of them are Very Sign from USA and Thawte Consulting from South Africa. Popular India CAs are SafeScrypt Ltd, TCS, IDRBT, MTNL Ltd and NIC.

Digital certificates contain the following:

Issuer, Issued to, organization name, organization unit, validity, Version, Public Keys, Thumbprint, algorithms etc.

Secure Socket Layer (SSL) is the widely used protocol for digital certificates. The Uniform Resource Locator (URL) starts with "https" instead of "http" and are secured by SSL. At the bottom of the window, a lock symbol appears for SSL. Generally, 128 bits SSL are used.40 bits SSL are also available.

Comparison between Electronic Signature and Digital Signature: (Aparajita Balaji, 2019, p.1)

Section 2 (ta) of Information Technology Act, 2000 had defined electronic signatures as:
"Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."

This definition has made the Act technologically neutral as it recognizes both digital and electronic signatures.

It is important to note that electronic signatures are not safe as they are not encrypted and are likely to be tampered unlike that of digital signatures which includes private key and public key for encryption and decryption.
Some of the commonly used electronic signatures are email signatures, web based signatures, digitized image of a signature. Therefore, it is advised that digital signatures should be used as they are more secure and have more legal weightage.

Electronic Signatures has no expiry or validity period unlike a digital signature which is valid up to a maximum of three years.

Electronic Signatures are used for verifying a document unlike digital signatures which is used for securing a document.

Section 2(1) (p) of Information Technology Act, 2000 had defined digital signatures as:
"Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."

Digital signatures are widely used for personal use, signing tenders, bidding, e-filing for ROC or income tax or for GST.

It follows an approach of using hash function i.e., usage of private key and a public key which is a two way protection system.

The process involves obtaining a digital signature certificate from a certifying authority which are set up and controlled by the mechanisms and law of the country. In order to transmit the message, public key and private key is used to encrypt and decrypt the message.

Check your progress 4 Spend 3 Min.

Is digital signature equivalent to handwritten signature legally?

2.8 AUTHENTICATION AND AUTHORISATION

Authentication is a term which is used (and often abused) in a very broad sense. By itself, it has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve. Examples of specific objectives include access control. The host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.

Authentication is one of the most important of all information security objectives. Until the mid 1970s it was generally believed that secrecy and authentication were intrinsically connected. With the discovery of hash functions and digital signatures, it was realized that secrecy and authentication were truly separate and independent information security objectives. It may at first not seem important to separate the two but there are situations where it is not only useful but essential. For example, if a two-party communication between Jack and Bond is to take place where Jack is in one country and Bond in another, the host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.

The preceding scenario illustrates several independent aspects of authentication. If Jack and Bond desire assurance of each other's identity, there are two possibilities to consider.

1) Jack and Bond could be communicating with no appreciable time delay. That is, they are both active in the communication in "real time".

2) Jack or Bond could be exchanging messages with some delay. That is, messages might be routed through various networks, stored, and forwarded at some later time. In the first instance Jack and Bond would want to verify identities in real time. This might be accomplished by Jack sending Bond some challenge, to which Bond is the only entity which can respond correctly. Bond could perform a similar action to identify Jack. This type of authentication is commonly referred to as *entity authentication* or more simply phrase challenge for *identification*.

For the second possibility, it is not convenient to challenge and await response, and moreover the communication path may be only in one direction. Different techniques are now required to authenticate the originator of the message. This form of authentication is called *data origin authentication*.

Thus, *Data origin authentication* or *message authentication* techniques provide to one for originality.

In the authentication process, verification of users is done and determines whether the person is a user or not while in the authorization process validation of users is done wherein determination is done as to whether the user has requisite permission to access the data or the information. Authentication is done prior to authorization process. The process of authentication requires user's login details while authorization only requires user's privilege or security levels. **(Geeks for Geeks, 2020,p.1)**

2.8.1 HASH FUNCTIONS

One of the fundamental primitives in modern cryptography is the cryptographic hash function, often informally called a one-way hash function simplified definition of hash function is given below.

Definition A *hash function* is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called *hash-values*.

The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed (using a publicly available hash function) and only the hash-value is signed. The party receiving the message then hashes the received message and verifies that the received signature is correct for this hash-value. This saves both time and space compared to signing the message directly, which would typically involve splitting the message into appropriate-sized blocks and signing each block individually. Note here that the inability to find two messages with the same hash-value is a security requirement, since otherwise, the signature on one message hash-value would be the same as that on another, allowing a signer to sign one message and at a later point in time claim to have signed another.

Hash functions may be used for data integrity as follows. The hash-value corresponding to a particular input is computed at some point in time. The integrity of this hash-value is protected in some manner. At a subsequent point in time, to verify that the input data has not been altered, the hash-value is recomputed using the input at hand, and compared for equality with the original hash-value. Specific applications include virus protection and software distribution.

A third application of hash functions is their use in protocols involving prior commitments, including some digital signature schemes and identification protocols.

Hash functions as discussed above are typically publicly known and involve no secret keys. When used to detect whether the message input has been altered, they are called *modification detection codes* (MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication as well as data integrity; these are called *message authentication codes* (MACs).

Some of the popular hash functions include: **(Tutorials Point, p.1**)

1) Message Digest is a 128-bit hash function which gives confidence about veracity of transmitted file. But it is no longer in practice as there were successful collisions i.e., analytical attack in 2004.
2) Secure Hash Functions family consists of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. The latest is Keccak algorithm which was chosen by NIST in October 2012 as the new SHA-3 standard which offers many benefits, such as efficient performance and good resistance for attacks.
3) The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was devised by open research community and generally known as a family of European hash functions.
4) Whirlpool is a 512-bit hash function which has stemmed from the revised edition of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.

2.8.2 Access control derivatives/ mechanisms

Definition A *cryptographic protocol* (*protocol*) is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Remark (*protocol vs mechanism*) As opposed to a protocol, a *mechanism* is a more general term encompassing protocols, algorithms (specifying the steps followed by a single entity), and non-cryptographic techniques (e.g., hardware protection and procedural controls) to achieve specific security objectives.

Protocols play a major role in cryptography and are essential in meeting cryptographic goals. Encryption schemes, digital signatures, hash functions, and random number generation are among the primitives which may be utilized to build a protocol.

Protocol and mechanism failure

Definition A *protocol failure* or *mechanism failure* occurs when a mechanism fails to meet the goals for which it was intended, in a manner whereby an adversary gains advantage not by breaking an underlying primitive such as an encryption algorithm directly, but by manipulating the protocol or mechanism itself.

Example (*mechanism failure*) Jack and Bond are communicating using a stream cipher.

Messages which they encrypt are known to have a special form: the first twenty bits carry information which represents a monetary amount. Active adversaries can simply XOR an appropriate bit string into the first twenty bits of cipher text and change the amount. While the adversary has not been able to read the underlying message, she has been able to alter the transmission. The encryption has not been compromised but the protocol has failed to perform adequately; the inherent assumption that encryption provides data integrity is incorrect.

Example (*forward search attack*) Suppose that in an electronic bank transaction the bit field which records the value of the transaction is to be encrypted using a public-key scheme. This simple protocol is intended to provide privacy of the value field – but does it? An adversary could easily take all possible entries that could be plaintext in this field and encrypt them using the public encryption function. (Remember that by the very nature of public-key encryption this function must be available to the adversary.) each of the cipher texts with the one which is actually encrypted in the transaction, the adversary can determine the plaintext. Here the public-key encryption function is not compromised, but rather the way it is used.

2.8.3 KEY ESTABLISHMENT, MANAGEMENTAND CERTIFICATION

This section gives a brief introduction to methodology for ensuring the secure distribution of keys for cryptographic purposes.

Definition *Key establishment* is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

Definition *Key management* is the set of processes and mechanisms which support key establishment and the maintenance of ongoing keying relationships between authorized parties, including replacing older keys with new keys as and when necessary.

Key establishment can be broadly subdivided into *key agreement* and *key transport*.

Many and protocols have been proposed to provide key establishment.

Key management encompasses techniques and procedures supporting:

1. initialisation of system users within a domain;
2. generation, distribution, and installation of keying material;
3. controlling the use of keying material;
4. update, revocation, and destruction of keying material; and
5. Storage, backup/recovery, and archival of keying material.

Key management through symmetric-key techniques

One solution which employs symmetric-key techniques involves an entity in the network which is trusted by all other entities. This entity is referred to as a *trusted third party* (TTP). Each entity shares a distinct symmetric key with the TTP. These keys are assumed to have been distributed over a secured channel. If two entities subsequently wish to communicate, the TTP generates a key (sometimes called a *session key*) and sends it encrypted under each of the fixed keys. This approach has certain advantages and disadvantages.

A symmetric cryptographic system is a system involving two transformations – one for the originator and one for the recipient – both of which make use of either the same secret key (symmetric key) or two keys easily computed from each other. An asymmetric cryptographic system is a system involving two related transformations– one defined by a public key (the public transformation), and another defined by a private key (the private transformation) – with the property that it is computationally infeasible to determine the private transformation from the public transformation.

Advantages

1. It is easy to add and remove entities from the network.
2. Each entity needs to store only one long-term secret key. Disadvantages

1. All communications require initial interaction with the TTP.
2. The TTP must store long-term secret keys.
3. The TTP has the ability to read all messages.
4. If the TTP is compromised, all communications are insecure.

Key management through public-key techniques

There are a number of ways to address the key management problem through public-key techniques. Each entity in the network has a public/private encryption key pair. The public key along with the identity of the entity is stored in a central repository called a *public file*.

Advantages of this approach include:

1. No trusted third party is required.

2. The public file could reside with each entity.

3. Only public keys need to be stored to allow secure communications between any pair of entities, assuming the only attack is that by a passive adversary.

The key management problem becomes more difficult when one must take into account an adversary who is *active* (i.e. an adversary who can alter the public file containing public keys).
Please answer the following Self Assessment Question.

Check your progress 5 *Spend 1 Min.*
Key establishment can be divided into _____ and key transport.

2.8.4 TRUSTED THIRD PARTIES AND PUBLIC KEY CERTIFICATES

Definition A TTP is said to be *unconditionally trusted* if it is trusted on all matters. For example, it may have access to the secret and private keys of users, as well as be charged with the association of public keys to identifiers.

Various third party services require different types of trust and competency in the third party. For example, a third party possessing secret decryption keys (or entity authentication keys) must be trusted not to disclose encrypted information (or impersonate users). A third party required (only) to bind an encryption public key to an identity must still be trusted not to create false associations and thereafter impersonate an entity. In general, three levels of trust in a third party T responsible for certifying credentials for users may be distinguished. Level 1: T knows each user's secret key. Level 2: T does not know users' secret keys, but can create false credentials without detection. Level 3: T does not know users' secret keys, and generation of false credentials is detectable

Definition A TTP is said to be *functionally trusted* if the entity is assumed to be honest and fair but it does not have access to the secret or private keys of users.

Public-key certificates

The distribution of public keys is generally easier than that of symmetric keys, since secrecy is not required. However, the integrity (authenticity) of public keys is critical.

Primary advantages offered by public-key (vs symmetric-key) techniques for applications related to key management include:

1) *Simplified key management*. To encrypt data for another party, only the encryption public key of that party need be obtained. This simplifies key management as only authenticity of public keys is required, not their secrecy. . The situation is analogous for other types of public-key pairs, e.g., signature key pairs.

2) *On-line trusted server not required*. Public-key techniques allow a trusted on-line server to be replaced by a trusted off-line server plus any means for delivering authentic public keys (e.g., public-key certificates and a public database provided by an un-trusted on-line server). For applications where an on-line trusted server is not mandatory, this may make the system more amenable to scaling, to support very large numbers of users.

3) *Enhanced functionality*. Public-key cryptography offers functionality which typically cannot be provided cost-effectively by symmetric techniques (without additional online trusted third parties or customized secure hardware). The most notable such features are non-repudiation of digital signatures, and true (single-source) data origin authentication.

A *public-key certificate* consists of a *data part* and a *signature part*. The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes). The signature part consists of the signature of a TTP over the data part.

2.8.5 PSEUDORANDOM NUMBERS AND SEQUENCES

Random number generation is an important primitive in many cryptographic mechanisms.

For example, keys for encryption transformations need to be generated in a manner which is unpredictable to an adversary. Generating a random key typically involves the selection of random numbers or bit sequences. Random number generation presents challenging issues.

Often in cryptographic applications, one of the following steps must be performed:

i) From a finite set of elements, select an element at random.

ii) From the set of all sequences (strings) of length over some finite alphabet of symbols, select a sequence at random.

iii) Generate a random sequence (string) of symbols of length over a set of symbols.

It is not clear what exactly it means to select at random or generate at random. Calling a number random without a context makes little sense. Is the number a random number?

A **Pseudo Random Number Generator** (**Geeks for Geeks, 2019, p.1**)

It refers to an algorithm that utilities mathematical formulation to create series of random numbers. They produce a series of numbers assessing the properties of random numbers.

With the arrival of technology, computer programmers acknowledged the requirement for a way of announcing unpredictability into a computer program. In spite of this, unexpected as it may seem, it is tough to get a computer to do something by chance as computer trails the specified instructions unseeingly and is therefore totally foreseeable. It is not possible to create truly random numbers from deterministic thing like computers so this is a method expounded to generate random numbers using a computer.

Some of the advantages are that this system is efficient as it can create number in a short span of time, easy to determine if replaying the same sequence of numbers again at a later stage and lastly are periodic i.e., that the sequence will eventually repeat itself.

2.9 PUBLIC KEY INFRASTRUCTURE/ DATA ENCRYPTION STANDARD

A PKI stands for Public key Infrastructure in cryptography. Development in PKI occurred in the early 1970s at the British intelligence agency GCHQ where James Ellis and Clifford Cocks made popular

development for PKI. The sole purpose of PKI is to facilitate the best secure electronic transfer of information for digital activities. It is an arrangement that binds public keys with respective identities of entities. The binding is established through a process of registration and issuance of certificates at and by a Certificate authority (CA).

The deployment of PKI may be delegated by a CA to assure valid and correct registration, which is called registration Authority (RA). The Internet Engineering Task Force's RFC 3647 defines an RA. So, the RA is responsible for accepting request for digital certificates and authenticating the entity requested by the user. The most unique feature of PKI is that it uses a pair of keys to achieve the secured digital communication by comprising both private and public keys.

Therefore, an anatomy of PKI comprises of the following components:

Public key certificate commonly referred as digital certificate (X 509 standard defines it)
Private key tokens
Certificate authority
Registration Authority
Certificate management System.

Data Encryption Standard:

DES (Data Encryption Standard) is a encryption algorithm which uses symmetric keys for cipher encryption. It uses 56 bits (+8 parity bits) in 16 rounds having a block size of 64 bits. It has been designed by IBM team and adopted by national Institute of standards of Technology (NIST). It was first published in 1975 (federal Register standardized in 1977. Its structure is Balanced Feistel Network and its successors are Triple DES, G-DES, DES-X, LOKO89 and ICE

TRIPLE DES is a symmetric key-block cipher which applies DES cipher in triplicate. It encrypts with first key (K1), decrypts with second key (K2) then decrypts with third key (K3). This is also a two-key variant where K1 and K3 are the same keys.

Though DES is no longer NIST's federal standard, it does not mean that it is no longer in use. Triple DES is still used today and it is considered a legacy encryption algorithm. But in practice, PKI has overcome the DES for ensuring digital communication system.

The main disadvantage of Public Key Infrastructure is that one of the keys i.e., public key is in a public domain and is therefore, likely to be misused. It is rarely seen that cryptographic schemes are compromised due to weakness in their design but very often it is compromised due to the poor key management. The same can be achieved by keeping private keys secret throughout. (**Tutorials Point, p.**1)

Let us now summarize the points covered in this unit.

2.10 SUMMARY

- Encryption is one common method of protecting information transmitted over unreliable lines where plain text is being converted to Cipher text and then again to plain text.
- Basically, there are two algorithms used for encryption. One is RSA and other one is DES.
- RSA is an asymmetric cryptography and DES is symmetric one.
- A system where one secret key shared is called Symmetric or Secret Key Cryptography.

- A cryptosystem where two different keys are used for encryption and decryption is called Asymmetric or Public Key System.

- Digital signature is a technique to secure electronic information in such a way that the originator of the information, as well as the integrity of information can be verified with proper authentication.

- Digital certificates are provided by Certified Authorities (CAs) to authenticate that a particular site is globally secured.

- There are five common CAs in India. They are Safescrypt Ltd, TCS, IDRBT, MTNL and NIC.

- A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length called hash-values. The most common cryptographic uses of hash functions are with digital signatures and for data integrity.

- Key establishment is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

- Key establishment can be subdivided into key agreement and key transport.

- Key management is the set of processes and mechanisms, which support key establishment and the maintenance of ongoing keying relationships between parties, including replacing older keys with new keys as and when necessary.

2.11 SOLUTIONS/ANSWERS

Check your progress

1) (i) Cipher text, (ii) Transposition

2) The advantages of Asymmetric keys are as follows:

   1. Only the private key must be kept secret

   2. The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP
   3. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time

3) RSA is asymmetric cryptographic algorithm and uses two different keys for encoding and decoding while DES is a symmetric cryptosystem and the cipher text is decrypted using the same key. It is a complex algorithm. So far no breaking of RSA has been reported though DES can be broken

4) According to Patrick W. Brown, Digital Signature technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital Signature technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as technology promises assurance at least equal to written signatures. From a legal

standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology are being created as the use of digital signature technology is adopted. Digital signatures may be used to provide assurances in distributed and networked computer environments where electronic transactions require a high degree of trust.

5) Key Agreement

2.12 REFERENCES/ FURTHER READINGS

- Aparajita Balaji (2019). Digital Signature and Electronic Signature as defined under the law. https://blog.ipleaders.in/digital-electronicsignature/#:~:text=Sec%202%20(ta)%20of%20Information,schedule%20and%20includes%20digital%20signature.%E2%80%9D
- Brown, P.W (1994). "Digital signatures: are they legal for electronic commerce".*Communications Magazine*. IEEE. 32.9: 76 – 80.
- Gary C. Kessler (2001), Steganography: Hiding Data Within Data, p1; https://www.garykessler.net/library/steganography.html
- Gary C. Kessler (2021), An Overview of Cryptography, p1; https://www.garykessler.net/library/crypto.html
- Geeks for Geeks (2020), Difference between Authentication and Authorisation, p1; https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/
- Geeks for Geeks (2020), Pseudo Random Number Generator, p1; https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/
- J. Quisquater and M. Girault (1990). 2*n*-bit hash-functions using *n*-bit symmetric block cipher algorithms. *Advances in Cryptology, Proc. Eurocrypt'89, LNCS 434*, J.-J. Quisquater and J. Vandewalle, Eds., Springer-Verlag, 1990, pp. 102–109.
- J. Wiener (1994). Efficient DES Key Search. *TR-244. School of Computer Science*, Carleton University, Ottawa, Canada.
- Jay Thakkar (2020). Types of Encryption. p1. https://www.thesslstore.com/blog/types-of-encryption-encryption-algorithms-how-to-choose-the-right-one/
- Mlen Milenkivic (1992). *Operating System Concepts and design*. New York: McGraw-Hill, Inc,.
- Peter Wayner (1995). Agents Unleashed: A Public Domain Look at Agent Technology.
- Silberschatz. Galvin, Gagne (2006). *Operating System Concepts*. 7th ed. John Wiley & Sons.
- The Economic Times (2021). Definition of Ciphertext. p1; https://economictimes.indiatimes.com/definition/ciphertext
- Tutorials Point. Cryptography Hash Functions. p1; https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
- Tutorials Point. Public Key Infrastructure. p1; https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm

UNIT 03 Data Security and Management

Structure

3.0 INTRODUCTION

The tremendous and intensive use of information for several different tasks makes data security, trustworthiness and privacy increasingly critical for these functionalities' in day-to-day living. The protection of data from unauthorised access, use, change, disclosure and destruction by using methods to ensure network security, physical security and file security based on a collection of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure is known as data security. Data security can be applied through various techniques and technologies including administrative controls, organizational standards, etc. and other safeguarding techniques that limit or preclude access to unauthorized or malicious users or processes.

The fundamental question which emerges from this extensive use of data is that why is it important to secure this data and how is this object to be achieved.

Different organizations create, collect, store, receive or transmit data within an organization as well as between organizations/associations and individuals or from one organization to an organization. It doesn't matter what device, technology or process is employed to manage, store, collect or distribute data, but it must be protected as data breaches may result in litigation and huge penalties alongside damage to an organization's reputation. Therefore, the importance of protecting data from security threats is more important today than ever before.

Threats to database are often numerous which can either be accidental or intentional and in either case security of the database and the entire system, including the network, operating system, the physical area where the database resides and the personnel access all have to be considered and protected accordingly.(**Sie Learning, Sydney, 2020, p.1**)

A data security plan which includes procedures both physical and virtual through extensive use of data management software is required to be put in place.(**Michael Buckee, 2020, p.1**)

3.1 OBJECTIVES

After studying this unit, you will be able to:

- Explain what is data security
- Explain data management
- Explain security requirements
- Explain security threats and attacks
- Security measures and usability
- Security management

3.2 Data security and Data Management

Database security is necessary in the following situations:

- Theft and fraud
- Loss of availability of data
- Loss of confidentiality
- Loss of data privacy
- Loss of data integrity

The situations given above are the most likely to be exposed to date security threats and are required to be protected so that the chances of losses in this regard can be significantly reduced.(**The National Academics Press, 1991, ch. 4, p. 49-73)**

It is noteworthy that these situations often cause cumulative losses due to inter dependencies and hence a loss due to one situation can affect multiple areas in the same organisation.

The purpose of data protection (also known as information privacy and data privacy) is to define when and under what circumstances data can be safely put to use

Data management

The main aim of data management helps people and organizations for data to be used within the boundaries of policies and regulations for the maximum benefit of these organizations and businesses and therefore is very valuable as an intangible asset. Data management can be achieved by the practise of collection, keeping and usage of data in a secure, efficient and cost-efficient manner.

Therefore, efficient ways and means are sought by various organizations for data management. The management of data is done through various platforms and include databases, data analysis and more such tools like Microsoft SQL server, Google cloud, Amazon web services, etc.

1. Data management is the responsible stewardship of data throughout its lifecycle. There are five components to data management:

- **Acquisition**
- **Utilization**
- **Maintenance**
- **Access**

- **Protection**

  Effective data management requires appropriate acquisition, utilization, maintenance, access, and protection of data. Data management depends on information confidentiality and criticality.

3.3 SECURITY REQUIREMENTS (CIA)

Data is being used by a vast majority of individuals, entities, businesses and organizations. One such example are the banking giants which deal with massive volumes of private and financial data to the one-man business storing the contact details of his customers on a mobile phone, data is at play in companies both large and small**.(Michael Buckbee, 2020, p.1**)

Since individuals, entities, businesses and organizations deal with data on an everyday basis, this data accumulated over time needs to be protected from outsiders with an intention to misuse such data. Therefore, data security is the primary aim for protection of such data.

Data security is necessary and importantin today's world for all devices or processes which deal with collection, management and storage of data as data breaches may occur anytime and can not only lead to litigation but also damage to the brand and reputation.

The core elements of data security are *confidentiality, integrity and availability*. Also known as the **CIA triad**, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access.(**Michael Buckbee, 2020, p.1**)

The three governing principles are as follows:

- **Confidentiality**
  Confidentiality or privacy refers to measures taken to ensure that data- particularly sensitive data- is protected from unauthorised access. Keeping in mind the age of ultra-modern technology, privacy is required to be a basic design consideration. The extent of level of confidentiality can vary based on the data type and/or regulation.

- **Integrity**
  Integrity pertains to safeguarding the accuracy of data as it travels through workflows. There should be measures taken to protectdata from unauthorized deletion or modificationand to quickly reverse the damage in the event of a breach. (**ShyamOza, 2019, p.1**)
- **Availability**
  Availabilitymeans providing seamless and continuous access to users through robust servers and network infrastructure with high availability mechanisms built into system design (**ShyamOza, 2019, p.1**).

Some practices for implementation of CIA Triad of confidentiality, integrity and availability are as follows:

i) Putting confidentiality into practice

- Categorization of data and assets being handled by individuals in an organization based on their privacy requirements.
- Requirement of all data encryption and two-factor authentication to be basic security hygiene as a fundamental practice in all organizations dealing with sensitive information.

- Ensure that access control lists and file permissions are monitored and updated regularly by professionals from the IT department in an organization.

ii) Scoping integrity

- Review all data processing, transfer and storage mechanisms and run diagnostic tests to ensure there is no unauthorised access.
- Understand organization's compliance and regulatory requirements by keeping in check with the rules and regulations updated.
- Invest in dependable backup and recovery solution; one that assures business continuity and quick data recovery in the event of a security or data breach.

iii) Ensuring availability

- Build preventive measures into system designs, make security audits routine, auto-update or stay alert of system, network and application updates.
- Utilize detection tools such as network/server monitoring software and anti-virus solutions and regular check-up through timely runs.

Check your progress1 *Spend 3 Min*

What is availability and integrity?

3.4 SECURITY THREATS AND ATTACKS

In today's day and age there is a host of new and evolving cyber security threats that has the information security industry on high alert. There is an increasingly more sophisticated cyber-attacks involving malware, phishing, cryptocurrency. Therefore, the data and assets of the corporations, governments and individuals are at constant risk.

The information technology industry suffers from a severe shortage of cyber security professionals and due to the ever-evolving new technology being introduced periodically, there has been an exponential rise in cybercrime.

The following cyber security threats are constantly growing and creating issues related to data privacy:

i) **Phishing attacks**- These are carefully targeted digital messages transmitted to fool people into clicking on a link that can then install malware or expose sensitive data. Nowadays everyone is aware of the risks of email phishing or of clicking on suspicious-looking links, leading to hackers upping their ante by distributing fake messages with the hope that the recipients will unwittingly compromise their network system. Such attacks enable hackers to steal user logins, credit card credentials and other types of personal financial information, as well as gain access to private databases.

ii) **Ransomware attacks-** Hackers deploy technologies that enable them to literally kidnap an individual or organization's databases and hold all of the information for ransom. These types of attacks are believed to cost victims billions of dollars every year.

iii) **Cyber-physical attacks**- The technology that has enabled to modernize and computerize critical infrastructure also brings risk. There is an ongoing threat of hacks targeting electrical grids, transportation systems, etc., which represent a major vulnerability.

iv) **State-sponsored attacks-** Hackers look to make profit through stealing individual and corporate data. Now even nation states use cyber skills to infiltrate other governments and perform attacks on critical infrastructure. Cyber crime today is a major threat not only to the private sector and individuals but also towards the governments and nations as a whole.
Many such attacks target government-run systems and infrastructure, but private sector organizations are also at risk.

Please answer the following Self-Assessment Question.

Check your progress2 *Spend 3 Min*

What are the various types of cyber threats?

3.5 COMPUTER, MOBILE AND INTERNET

The computer is the foundation of the entire virtual world and is now extensively used both personally and professionally in all walks of life. As the technology related to computers is constantly developing, the methods to secure data within the computers is not necessarily progressing a same pace. The computer inturn has given rise of many other forms of communication which includes the mobile.

The mobile from its name itself denotes communication on the move. This has actually made many conventional systems of interaction obsolete. However due to its ease of use certain issues of data security have surfaced from time to time.

The Internet is an international network of computer systems that has evolved over the last decade. Currently, the Internet interconnects several thousand individual networks that connect over a million computers. The Internet today has become the electronic backbone for computer research, development and user communities. Similar issues of data security which affect the computer and mobile also affect the Internet.

COMPUTER

A computer in layman terms is essentially a machine that was primarily used for calculations. Over the years, the use of a computer has grown two-fold; it not only helps in storing work related information but also has the capacity to transfer communication from one system to another with the help of the Internet.

Computers today have reduced complicated jobs into much simpler tasks. For example, one can write a letter in a word document, edit it, spell check, print copied and also send it to someone across the world in a mere matter of seconds. These activities of simply even writing a letter would have taken someone days, to do before the advent of computers.

In other words, a computer simply is an information processor in a way that it takes whatever raw information or data which is fed by a human and stores that information, then proceeds to decrypt the information entered and consequently provide the result in the form of an output.

The work of a computer is nothing without a computer program. We can see various computer programmes on a computer we rely on like Microsoft Word, Excel, etc. used for carrying out day to day activities at all spheres of life.

MOBILE

The world of digital technology has led to the evolution of various devices that are used for day to day purposes. A computer system is one that cannot be carried by an individual to every place. Therefore, foreasy use of electronic devices and to avail benefits of a computer system a mobile was invented.

A mobile device in essence is a general term used for a handheld computer or a smartphone. The mobile devices invented not only has functions of making calls, receiving calls, sending and receiving text messages, but all contains functions of obtaining emails and carries out functions of a computer system at a smaller level.

A mobile as per defined by digital technology refers to a cell phone usually one with computing ability, or a portable, wireless computing device used while held in the hand, as in mobile tablet, mobile, mobile app, etc.

The success of a mobile's technology has risen in today's world due to possession of a smartphone which has access to Internet and can be used to connect to multiple users wherever and whenever required.

Characteristics of a mobile device (Priya Viswanathan, 2019, p.1):

- Wi-Fi or cellular access to the Internet
- A battery that powers the device for several hours
- A physical or onscreen keyboard for entering information
- Touch-screen interface
- Ability to download data from the Internet

Different meanings of mobile

In different contexts, mobiles are also defined as "mobile development", "mobile-friendly", etc. The term "mobile development" usually refers to creating apps for smartphones, but does not include laptops. "Mobile friendly" on the other hand refers to websites that are easy to use by any user owning a smart phone.

INTERNET

Merriam-Webster's dictionary defines Internet as *an electronic communications network that connects computer networks and organizational computer facilities around the world*.(**Merriam-Webster Dictionary, 2020, p.1**)

There are various devices that help facilitate connections with people around the world with the help of a network. These multiple interconnected networks form the Internet.

How does a user access the Internet?

The answer is simple. A single device that is assigned with an address when it connects to the Internet known as the Internet protocol (IP) address and this address helps in differentiating between devices in the network form all other devices.

Almost every connection to be made with the Internet requires a device which includes an address for sending/receiving messages in the form of emails. Mobile phones too, operate within a network based on services that are provided by service providers. They convert our voice into electronic signals which are then transmitted through radio waves. The same then get converted back into a sound once it reaches another mobile phone.

The use of Wi-Fi has grown two-fold due to connection to the Internet wirelessly. The concept of free Wi-Fi is now commonly available in public places such as airports, cafes, etc.

3.5.1 LIMITATIONS

Like every technology that has advanced every day, the risks too increase. Even a mobile phone/device and a computer having an Internet technology has its limitations. Some of them are mentioned below:

- Speed- Speed of the Internet is very essential for complete usage of a mobile device. If the speed of an Internet connection is slow, it results in lagging or slows down of the device and crashes which then renders the mobile device unusable.
- Accessibility- Websites though easily accessible on laptops may not be easily accessible on a mobile device as the website may not have implemented mobile versions. Therefore, a mobile phone may not always get the desired website to be accessed by a user.
- Incompatibility- Mobile web browsers are not the same as a laptop or a computer web browser works. Therefore, some web browsers may be incompatible with mobile operating systems.
- Leakage of data- Mobile apps often provide free apps in the form of advertisements, which usually do not undergo malware tests to ensure safety of the app. Therefore, users downloading such mobile apps make themselves liable to unintentional data leakages relating to personal data.
- Use of unsecured Wi-Fi- Users of internet want to preserve their cellular data for the long run or to not receive hefty phone bills and therefore rely on free Wi-Fi networks. At time such free Wi-Fi network are unsecured and leads to compromise of data security which is liable to be hacked by technology users.
- SMishing- This type of scam is similar to the phishing scam wherein cybercriminals ask users to download malware by clicking on malicious links. The method of SMishing scam is done through text messages instead of email like in the case of phishing scams.

3.6 SECURITY MEASURES AND SOLUTIONS

As discussed on 3.3 which deal with security requirements, it has been stated that the concept of CIA is very important. Further, security threats are inventive according to the new information technology launched. These security threats constantly evolve and are harmful to an organization as they steal, harm or corrupt information stored in an organization's system. An organization should arm themselves with resources to safeguard themselves from the ever-growing security threats. Therefore, the CIA triad though being a security model and guide for organizations to protect their sensitive data there are a few other data security considerations that one should be aware of:

- **Access security**- By restricting access of users who have been granted access to information, thereby results in monitoring who all have access to a particular data. Therefore, in cases of data theft, sifting through the timelines of access granted to users can be easier to track down the culprit.

- **Data encryption**- Data when kept unencrypted leads to misuse of personal data by cybercriminals. Therefore, data has to be encrypted by usage of unique encryption codes, so as to avoid leakage of vital information stored in databases. When data has been encrypted and only the user has access to such a data has the decryption code, results in prevention of data theft.

- **Email security**-It is a form of procedure to protect an email account and the contents on an email account from unauthorised access. Therefore, measures like strong email passwords, end-to-end encryption of emails or messages that are sent from one person to another result in prevention of misuse of data, as emails are a popular forum for hackers to spread malware, spam and phishing attacks. For example- end-to-end encryption used by WhatsApp.

- **Risk-assessment analysis**- Organizations have to take a proactive approach while dealing with information security concerns. The main of conducting a risk assessment is to identify the risks pertaining to information stored in an organizations system. By conducting risk assessment analysis, an organization can understand and assess internal and external risks to their security, confidentiality and personal information stored in various storage media like laptops and portable devices.

- **Monitor effectiveness**- It is critical for an organization to verify security programs established and to establish if such security programs manage cyber security measures implemented for safeguarding an organization's information or data. This is done through regular tests and monitoring of information security programs annually or quarterly helps to assess the number of attacks made to an organizations data.

- **Third party issues**- Website's play a major role while showcasing an organization's success. Therefore, they implement third party tools to make their websites' more interactive and user-friendly and offer smooth connectivity for user interaction. These third-party tools help in generating revenue for an organization's website. Therefore, an organization has to undertake to ensure that all reasonable steps have been taken prior to giving access to third party service providers and that such third-party service providers apply the stringiest security measures.

- **Strong firewall**- Firewall of a system is part of such system's cyber security measure. A firewall enables to protect a system from internet traffic and services it is exposed to. These services are accessed by everyone who uses an internet. Therefore, firewalls enable to control who gains access to an organization's system like insider attacks which may originate from within a network used by an organization. Antiviruses are for files and firewalls are needed to protect from unauthorised access or usage of network. A firewall simply helps to control Internet traffic that is generated by using a network for work.

- **Antivirus protection**- An antivirus protection can be gained in the form of antivirus software. This software is a program designed to avoid, detect and deal with cyber

security threats that an organization may face. The process of an antivirus is to run background scans on a system to detect and restrict unauthorised access in the forms of malware and to protect a system from vulnerabilities it may face. These solutions are extremely important for data security and must be installed on computer systems. These antivirus protections are available not only for laptops and computers but also for mobile devices and help to fight unwanted threats to files and data.

- **Back-up regularly-** A data security is meant for protecting information stored on a system from unauthorised access, destruction of such information and includes network security. Therefore, to avoid loss of data, data should be regularly be stored and kept somewhere safe where it cannot be accessed or violated by anyone. Further, the securing of such data helps in preventing accidental modification to data, theft of data, breach of confidentiality agreements and avoid release of data prior to its verification and authentication.

Check your progress3 *Spend 3 Min*

Describe in brief the various security measures.

3.7 SECURITY POLICY

In 2013, the Government of India took the primary formalized step towards cyber security vide Ministry of Communication and Information Technology, Department of Electronics and Information Technology's National Cyber Security Policy, 2013.

The purpose of the policy is to create a safe and resilient cyber space for individuals, organizations and the government. The mission is to secure cyberspace data and framework, develop capacity to avert and react to cyber-attacks and mitigate harm through collaboration of institutional systems, individuals, procedures and technology.

Some of the strategies adopted by the policy include (Government Initiatives, 2013):

- Creating an assertion structure;
- Encouraging open standards;
- Strengthening the administrative structure combined with intermittent audits, synchronization with global guidelines and spreading awareness about the legitimate system;
- Securing e-administration by executing worldwide accepted procedures and more extensive utilization of Public Key Infrastructure.

In India, the government recently implemented some essential tools to resolve cyber security issues as mentioned below:-

1. USB Pratirodh was launched by the government to monitor unauthorized use of removable USB storage media devices.
2. Samvid permits just pre-approved set of executable documents for execution and shields work areas from suspicious applications from running.
3. M-Kavach gives insurance against issues identified with malware that take individual data and accreditations, abuse Wi-Fi and Bluetooth assets, misplaced or stolen versatile gadget and undesirable/spontaneous approaching calls.

Browser JSGuard is a device which fills in as a program augmentation which distinguishes and protects malicious HTML and JavaScript attacks. It warns the user while visiting malicious web pages and provides a comprehensive threat analysis report of the web page.

3.8 SECURITY MANAGEMENT

Security management means minimizing the interruption of business activities and reducing the vulnerability to various attacks. Security bargains with distinctive trust aspects of information.

Data security includes engineering where an incorporated permutation of appliances, arrangements and resolutions, software, surveillance, and vulnerability scans work together.

Security is not just restricted to computer systems; it applies to all perspectives of securing data or information, in whatever structure. Security is accomplished utilizing a few methodologies at the same time or utilized in blend with one another.

There are six principles of security management:-

1. Availability- The continuous accessibility of systems tends to procedures, policies and controls which are used to ensure prompt access to data for authorized customers. This purpose secures against deliberate or inadvertent endeavours to refute legitimate costumers' access to data.

2. Integrity of data or systems- System and data integrity is linked to the procedures, policies and controls which are used to guarantee that data has not been modified in an unconstitutional way and that systems are liberated from illicit manipulation that would compromise precision, comprehensiveness and consistency.

3. Confidentiality of data or systems- Confidentiality covers the procedures, policies and controls which are utilized to secure data of customers and the organization against illicit access or use.

4. Accountability- Accountability incorporates the procedures, policies and controls essential to follow activities to their source. Accountability specifically underpins non-repudiation, anticipation, infringement, deterrence, security checking, recuperation and legitimate tolerability of records.

5. Assurance- Assurance addresses the procedures, strategies and controls which are used to create certainty that specialized and equipped security measures are working as anticipated.

6. Privacy- It centres on the constitutional rights of people, the motivation behind data assortment and processing, security predilection and the manner in which organizations administer individual's data. It focuses on how to gather, process, offer, document and erase the information/data as per the law.

3.9 SECURITY AUDIT

Security auditing is a vital part to assess the security strength of data frameworks and systems for any organization and in this way the determination of the foremost suitable

security auditor could be an important choice. Due to its exceptionally particular and specialized nature, security examination is often outsourced.

Considering the inclusion of sensitive, critical and private organizational information, it is imperative that security evaluator should be competent and reliable. Security inspecting assignments can take numerous diverse shapes depending upon the sort and measure of auditee organization. It is recommended that audit contracts be settled only upon discussion with auditee's officially authorized/contractual specialists and after consultation with the auditor. Security auditing under the risk management plan may be conducted as a separate task or as part of the risk assessment process.

Security audits give a reasonable and computable way to scrutinize how secure a site really is. This assessment is designed to:-

- Create a security benchmark for your organization;
- Identify the qualities and shortcomings of current security rehearses;
- Prioritize the exposures that present the most serious hazard;

Provide hazard alleviation proposals reliable with consistence guidelines, security industry best practices, customer industry best practices and customer business targets. The information picked up from data security audits enables customers to make more informed resolution about how to allot budgets and assets so as to most viably oversee hazard.

Check your progress4 *Spend 3 Min*

Describe security audit?

3.10 SECURITY AND USABILITY

Reliance on information technology in the society has been increasing by leaps and bounds with the resulting ability of organizations, individuals to conduct attacks on computer systems, networks, mobiles, etc.

Computer security in layman terms is defined by the attributes of the CIA triad.

The term usability can be taken in narrow terms of quality of a system's interface, but the concept applies more broadly to how a system supports the requirements of the user. Usability though dealing with quality of a system's interface also includes the term "user experience". This refers to the ease with which a user can access or use a product or a website.

The official ISO 9241-11 definition of usability is: *"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."* **(Interaction Design Foundation, 2020, p.1)**

Thus, usability deals with the following outcomes:

- A website or product should be easy for a user, so that they can navigate such websites without unnecessary hindrances and work with efficiency;
- A user can achieve their objectives through using a particular website by way of easy and detailed navigation. For example: the process of booking a movie ticked, if a good design is in place, it will guide the user through the easiest process to purchase movie tickets;

– A user upon subsequent visit to a website or a product page can easily recall and use such website or product page.

Usability though dealing with quality of a system's interface also includes the term "user experience". This refers to the ease with which a user can access or use a product or a website.

Many advances have been made towards security but it often remains complex and has to be managed effectively or conveniently by individuals or enterprises. Security is hard to understand and thereby often results in use of operating systems in an unsecured manner. Therefore, security technologies have been developed in such a manner wherein system administrators have primary responsibility of maintaining security protection.

Though security protections have been enhanced in various ways to protect a data system from malicious attacks, at times such security protections tend to be clumsy and awkward, resulting in obstacles to get work done resulting in security protections being disabled or bypassed by users. This leads to end users often engaging in actions, knowingly or unknowingly compromising the security of computer systems or contribute to attacks by hackers. Therefore, security and usability are attributes that trade off against each other. Usability decides if protection of a system is strong or not.

3.11 SUMMARY

The protection of data from unauthorised access, use, change, disclosure and destruction by using methods to ensure network security, physical security and file security based on a collection of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure is known as data security. Data security can be applied through various techniques and technologies including administrative controls, organizational standards, etc. and other safeguarding techniques that limit or preclude access to unauthorized or malicious users or processes.

Database security is necessary for the following situations:

- Theft and fraud
- Loss of confidentiality or secrecy
- Loss of data privacy
- Loss of data integrity
- Loss of availability of data

In some conditions, these areas are directly related such that an activity that results in a loss in one area can also cause a loss in another since all of the data within an organization are interconnected.

Data management is the practice of collecting, keeping and using data securely, efficiently, and cost-effectively. The goal of data management is to assist people, organizations and connected things optimize the use of data within the bounds of policy and regulation in order that they will make decisions and take actions that maximize the benefit of the organization.**(Oracle, 2020, p.1)**

The main objective of data security is to protect the data which an organization directly owns or that which belongs to third party while this data is being received, collected, stored created or shared, as the case maybe.

There is no difference as to which device, technology or process is utilized to manage, store or collect data, and it must be protected. Data breaches may result in litigation cases and huge

fines, but it may also lead to damage an organization's reputation. The importance of shielding organizations, individuals and business' data from security threats is more important today that it's ever been.

The core elements of data security are *confidentiality, integrity and availability*. Also known as the **CIA triad**, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration. (**Michael Buckbee, 2020, p.1**)

The information technology industry continues to suffer from a severe shortage of cyber security professionals and experts constantly warn that the stakes are higher than ever. The rise in cybercrime epidemic even risks shaking the public faith in such cherished ideals as democracy, capitalism and personal privacy.

The following cyber security threats are on the rise and posing a risk to data privacy:

i) Phishing attacks
ii) Ransomware attack
iii) Cyber-physical attack
iv) State-sponsored attack

The CIA triad though being a security model and guide for organizations to protect their sensitive data there are a few other data security considerations that one should be aware of:

- Access security
- Data encryption
- Email security
- Risk-assessment analysis
- Monitor effectiveness
- Third party issues
- Strong firewall
- Antivirus protection
- Back-up regularly

Security management means minimizing the interruption of business activities and reducing the vulnerability to various attacks. Security bargains with distinctive trust aspects of information.

Data security includes engineering where an incorporated permutation of appliances, arrangements and resolutions, software, surveillance, and vulnerability scans work together.

3.12 SOLUTIONS/ANSWERS

Check Your Progress

1. Integrity is the protection against proper modification or destruction of information includes non-repudiation and authenticity. Low integrity leads to concerns and information with high integrity is considered critical. Availability refers to the reliability, access to and use of information. Low availability of information may be considered supplementary whereas, high availability information is considered as critical and must be made accessible in order to prevent negative impact on an organization's activities.

2. The cyber crimes are:
   i) Phishing attacks which enable hackers to steal user logins, credentials and personal financial information to gain access to private databases;

ii) Ransomware attacks are used to kidnap an individual/organization's database for ransom purposes;
iii) Cyber-physical attacks are threats to electrical grids, transportation systems etc. to critical infrastructure;
iv) State sponsor attacks are used to infiltrate other governments and attack their critical information.

3. These are:
   i) Data encryption to ensure that personal data cannot be obtained illegally and be misused by cyber criminals;
   ii) Email security by end-to-end encryption so that only authorised individuals can access encrypted data;
   iii) Strong firewalls to protect from unauthorised access/usage of network;
   iv) Antivirus protection to protect data;
   v) Regular back-up to ensure that data is not lost or cannot be accessed by unauthorised individuals.

4. Security audit deals with regular inspection of security measures implemented to protect personal information. A security audit is conducted to give a reasonable way to scrutinize how secure a site is and/or the information stored is also properly protected. Security audit creates benchmarks for an organization to handle the shortcomings to security measures which have been implemented.

3.13 REFERENCES /FURTHER READINGS.

- Ashutosh Bhatt (2014). How Internet Works on Mobile Devices. p1-11; https://www.engineersgarage.com/how_to/how-internet-works-on-mobile-devices/
- Business Technology Standard. Security and data protection. p1-6; https://www.managebt.org/book/strategy-and-governance/security-and-data-protection/
- Circadence (2020). The future of finance cyber security in 2020. p1-3; https://www.circadence.com/blog/the-future-of-finance-cyber-security-in-2020/
- Denis Otieno (2020). Cyber security threats and trends for 2020. p1-14; https://just40days.com/detail_Cybersecurity-Threats-and-Trends-for-2020_37750
- Elisa Bertino (2016). Introduction to Data Security and Privacy, p1-6; https://link.springer.com/article/10.1007/s41019-016-0021-1
- Forcepoint. What is Data Security? Data security defined. explained and explored. p1-6; https://www.forcepoint.com/cyber-edu/data-security
- Government Initiatives (2013). https://baliyans.com/courses/disaster-management-and-internal-security/cyber-security/government-initiatives http://sielearning.tafensw.edu.au/toolboxes/Database_Administration/content/security/threats.htm
- Interaction Design Foundation (2020, p.1). https://www.interaction-design.org/literature/topics/usability
- Internet. https://www.merriam-webster.com/dictionary/Internet
- Makerere University. Data Security and Its Technologies. p1-3; https://answers.mak.ac.ug/security/data-security-and-its-technologies

- Michael Buckbee (2020). Data Security: Definition. Explanation and Guide. p1-12;.https://www.varonis.com/blog/data-security/
- Oracle India. What is data management?p1-10; https://www.oracle.com/in/database/what-is-data-management/
- Priya Vishwanatha (2019). What is a mobile device?. p1-11; https://www.lifewire.com/what-is-a-mobile-device-2373355
- Priya Viswanathan (2019. p.1). https://www.lifewire.com/what-is-a-mobile-device-2373355
- ShyamOza (2019, p1). CIA Triad: Best Practices for Securing Your Org.https://www.business2community.com/cybersecurity/cia-triad-best-practices-for-securing-your-org-02232416.
- ShyamOza (2019. p.1). https://spanning.com/blog/cia-triad-best-practices-securing-your-org/
- Sie Learning, Sydney (2020). Threats to the Database.
- The National Academics Press (1991). *Computers at Risk: Safe Computing in the Information Age*. Ch-4. 49-73; https://www.nap.edu/read/1581/chapter/4
- Unitag. What is mobile web?. P1-4. https://www.unitag.io/mobile-websites/
- W3Schools. Database Security. p1-2; https://www.w3schools.in/dbms/database-security/