Dr. AMBEDKAR INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, affiliated to VTU, Belagavi and Aided by Government of Karnataka)

Near Jnana Bharathi Campus, Mallathahalli, Bengaluru-560056

SEMINAR REPORT ON

"Cyber Security"

Submitted in partial fulfillment of the requirements for the award of the

BACHELOR OF ENGINEERING(B.E.) IN

COMPUTER SCIENCE & ENGINEERING

Submitted by

<u>SUBMITTED BY</u>

AARJEYAN SHRESTHA	**[1DA18CS001]**
ADARSH KUMAR DUBEY	**[1DA18CS006]**
AMIT CHAUDHARI	**[1DA18CS012]**
APIL BIST	**[1DA18CS021]**

Under the Guidance of
Mr. Chidanandan V
Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

2021-2022

Dr. AMBEDKAR INSTITUTE OF TECHNOLOGY

[An Autonomous Institution, affiliated to VTU, Belagavi and Aided by Government of Karnataka]
Near JnanaBharathi Campus, Mallathahalli, Bengaluru-560 056

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that this seminar report entitled **"Cyber Security"** by **AARJEYAN SHRESTHA[1DA18CS001], ADARSH KUMAR DUBEY[1DA18CS006], AMIT CHAUDHARI[1DA18CS012], APIL BIST[1DA18CS021],** submitted in partial fulfillment of the requirements of the 8th semester seminar for the degree of Bachelor of Engineering in Computer Science & Engineering of Dr. Ambedkar Institute of Technology, Bengaluru, during the academic year 2021-22, is a bonafide record of work carried out under my guidance and supervision.

Signature of guide	**Signature of HOD**	**Signature of Principle**
________________	________________	________________
Mr. Chidanandan V	Dr. Siddaraju	Dr. M. Meenakshi
Asst Prof, Dept of CSE	Prof & HOD of CSE	Principal
Dr. AIT	Dr.AIT	Dr. AIT

ACKNOWLEDGEMENT

The satisfaction that accompanies to this report would be incomplete without the mention of the people who made it possible, without whose constant guidance and encouragement would have made our efforts go in vain.

We consider ourselves privileged to express our gratitude and respect towards all those who guided us through the seminar of **, "Cyber Security".**

We consider ourselves proud to be part of **Dr. Ambedkar Institute of Technology,** the institute which stood by us throughout our endeavour career.

We would like to express our gratitude to **Dr. M. Meenakshi, Principal, Dr. AIT**, for providing us the congenial environment to work in.

We would like to express our profuse gratitude to **Dr. Siddaraju, HOD, Dept. of Computer Science and Engineering, Dr. AIT,** for giving us the support, encouragement and providing us the required lab facilities that was necessary for the completion of this project.

As a token of gratitude, we would like to acknowledge our sincere gratefulness to our seminar guide **Mr. Chidanandan V, Assistant Professor, Dept. of CSE, Dr. AIT** for the support and encouragement provided throughout the process.

We also express our gratitude and sincere thanks to all the teaching and non-teaching staff of **Computer Science and Engineering Department.**

Finally, yet importantly, we would like to express our heartfelt thanks to our beloved Parents for their blessing and our Friends for their help and wishes for the successful completion of this seminar.

[1DA18CS001], [1DA18CS006],
[1DA18CS012], [1DA18CS021]

Abstract

The Cyber Security plays a vital role in the area of information technology for safeguarding the information of individuals or government entities etc. This become an major concern in the current day. Cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrong doings. Beside various measures cybersecurity is as a significant worry to many. Our seminar report mostly emphases on cyber security and cyber terrorism. The cyber-terrorism could make associations lose billions of dollars in the region of organizations. Our seminar report also explains the components of cyber terrorism and motivation to such attacks. A Research paper and three case studies related to cybersecurity is also provide in this report . Some solution about cyber security and cyber terrorism is also explained briefly.

TABLE OF CONTENTS

Chapter 1

Introduction

The World is going on the digitalization or cashless transaction so multi-fold that even the government and defense organization have experienced significant increase in cyber thefts and disruptions. The crime environment in cyber space is different from the real space that is why there are many hurdles to enforce the cybercrime law as real space law in any society. For Example, age in real space is a self-authenticating factors compare to cyberspace which is not self-authenticating. A child under age of 18 can easily hide his age in Cyber space and can access the restricted resources where as in real space it would be difficult for him to do so. Cyber security involves protecting the information by preventing, detecting and responding to cyber-attacks.The penetration of computer in society is a welcome step towards modernization but needs to be better equipped to keen competition with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered arise difficulty for the security professionals in order to find hackers. The defense mechanism mainly concerns with the understanding of their own network, nature of the attacker, inspire of the attacker, method of attack and security weakness of the network to mitigate future attacks. The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is the companies that provide cloud computing do that and only that so these companies will be extremely well secured with the latest in cutting edge encryption technology.

How Cyber security is introduced?

Cyber security has become the important topic in today's generation of computers. Companies today often work to minimize cyber attacks to keep consumer and business data, high risk information, and much more safe. But there was a time when people knew so much about internet and cyber security. So where did cyber security start?

Cybercrime has evolved significantly since the first computers went online and started communicating with each other. The level of risk faced today is significantly more than it was then. As technology improves, so may cyber threats. The criminals in the industry often continue to develop new ways to infiltrate and gather information.

Many may think cybercrime began in the last few decades. Yet, computer systems have suffered vulnerabilities for much longer. In early 1940s, the first digital computer was created. There was no inter connection network and had no connection between computers to move data or files. In the late part of the decade , John von Neumann came up with a theory that some type of "mechanical organism" could occur and damage machines. It could copy itself like a naturally occurring virus. This was written by him and published in Theory of Self Reproducing Automata.

In 1950s the trend called phone phreaking began. Phone phreaks are people who attempted to hijack the protocols in place that enabled engineers to work on the network from a distance. This enabled people to make no cost calls and reduced tolls for long distance calling. This was the early sign of "Hacking" but the term Hacking was not developed till this decade.

In 1960s the term hacking developed when a group of people hacked the MIT Tech Model Railroad Club high tech train sets to make adjustments to their functionality.Still hacking and gaining access to these early computers didn't seem like "big business".

Over the time new faster and more efficient ways of hacking developed. In 1967, IBM welcomed a group of students into their offices to try out a newly designed computers.They learned about the computer system language and gained access to various parts of the system. This provide IBM with insight into vulnerabilities of the system. The result was the development of a defensive mindset, that computers required security measures to keep hackers out. This was the first example of ethical hacking in the industry.

The true birth of cybersecurity occurred in the 1970s. This began with a project called The Advanced Research Projects Agency Network (ARPANET).A man named Bob Thomas determined it was possible for a computer program to move over a network. He developed the program that could move between the Tenex terminals on ARPANET. He called this program CREEPER which would leave a simple message. “I’M THE CREEPER: CATCH ME IF YOU CAN.”

This sparked a lot of interest and some concerns.To chase and delete Creeper, Ray Tomlinson developed a new program called Reaper that would be the first example of an antivirus software program. That made Reaper the world’s first computer worm.

As the computer technology continued to grow and expand that placed a new, higher level of demand on ways to secure networks. Governments began discussing ways to reduce these vulnerabilities. The Electronic Systems Division (ESD) of the U.S. Air Force Command began working on projects. The Advanced Research Projects Agency (ARPA) was also involved. Other organizations began working on network security as well. That includes Stanford Research Institution and UCLA.

The Protection Analysis Project form ARPA was a key component of development. It looked at a wide range of topics. This includes identifying vulnerabilities. It worked on various aspects of OS security.

In 1979, just as the decade was waning, the first cyber criminal was arrested. His name was Kevin Mitnick(16 years old). He managed to hack into The Ark. The Ark was a massive system that was used for developing operating systems. Mr. Mitnick manged to make copies of the software after gaining access to it.

With the advent of cyber attacks present 1980s brought numerous problems for computer networks. Number of high profile attacks would take place in this decade. That includes attacks on AT&T, the Los Alamos National Laboratory and National CSS. It was in 1983 the new terms were developed to describe these attacks. Among them were “Computer virus” and “ Trojan Horse.”

In this way the attacks of viruses and malware became common the the following years. Different attackers or Hackers were created . 2000 became the growth of different such problems. First hacker group called Anonymous was developed at this time. Credit card hacks in 2000s , Yahoo attacks(2013 and 2014), SONY hacks, were one of the many cyber crimes that occurred in 2000s.

While this continued to be an error or intensifying threats, solutions developed, too. New detection methods developed. New solutions for unprecedented threats were created. This included the use of new technology and approaches. Some examples include:

- Computer forensics
- Multi factor authentication
- Network Behavioral Analysis (NBA)
- Real time protection
- Threat intelligence and updated automation
- Sandboxing
- Back up and mirroring
- Multi vector attacks
- Social engineering
- Web application firewalls

The threats from cyber attacks are numerous. They continue to be present. Phishing, personal data loss online, and ransomware attack events take place around the world often. Yet, finding a way to minimize security breaches has become more important than ever.

Reasons to introduce the cyber security?

It can be rightfully said that today's generation lives on the internet, and for a hacker, it's a golden age. With so many access points, public IP's and constant traffic and tons of data to exploit, black hat hackers, are having a great time exploiting vulnerabilities and creating malicious software for the same. Above that, cyber-attacks are evolving by the day. Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffles many people.Therefore there has to be some sort of protocol that protects us against all these cyberattacks and makes sure our data doesn't fall into the wrong hands. This is exactly why we need cybersecurity.

Cybersecurity is important because it protects all categories of data from theft and damages. This includes sensitive data, personally identifiable information(PII), protected health information(PHI), personal information, intellectual property, data, and governmental and industry information system.Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

Both inherent risk and residual risk are increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber attack or data breach is on the rise.

Business leaders can no longer solely rely on out-of-the-box cybersecurity solutions like antivirus software and firewalls, cybercriminals are getting smarter and their tactics are becoming more resilient to conventional cyber defenses. It's important to cover all the fields of cybersecurity to stay well-protected.

Cyber threats can come from any level of your organization. Workplaces must include cybersecurity awareness training to educate staff about common cyber threats like social engineering scams, phishing, ransomware attacks, and other malware designed to steal intellectual property or personal data.

Cybersecurity is not just relevant to heavily regulated industries. Even small businesses are at risk of suffering irrecoverable reputational damages following a data breach. Thus, Cybersecurity plays a vital role in today’s generation as it protects us from different cyber attacks, hacks, malware and unwanted problems regarding the computers and computer networks.

Chapter 2

Literature survey

The work in paper[1] focus on the importance of knowledge of what cyber security is and how to use it effectively . Systems, important files, data, and other important virtual things are at risk if there is no security to protect it. Whether it is an IT firm not, every company has to be protected equally. With the development of the fresh technology in cyber security, the attackers similarly do not collapse behind. They are consuming better and enhanced hacking techniques and aim the weak points of many businesses out there. Cyber security is essential because military, government, financial, medical and corporate organizations accumulate, practise, and stock unprecedented quantities of data on PCs and other devices. An important quota of that data can be sensitive information, whether that be financial data, intellectual property, personal information, or other various kinds of data for which illegal access or acquaintance could ensure negative concerns.

Technical paper/work referred

In this project [1] , different types of cyber security attacks and how various goals or objectives of cyber security to defend the data from these cyber security attacks such as phishing, malware, ransomware and social engineering makes working on the internet easy and safe for the people. It shows how confidentiality guarantees that your data is accessible to the user and data privacy is maintained, how integrity makes sure all your data is precise and how availability makes sure all your data is accessible at any given time. It lists important steps to maintain these goals.

2.1 Case Study Examples

2.1.1 Cyber Security in E-Governance case study [2]

E-Governance is the extension of the efforts completed through the governments to recover relations with their nationals. With its instilled straightforwardness and receptiveness, given the standards of the Internet, E- Governance conveys governments all the more near their residents. Existing and potential dangers in the circle of cybersecurity are among the most genuine difficulties of the 21st century. To ensure E-Governance extends there is a requirement for data security best practices (Hua, & Bapna, 2013). Security policies, practices, and techniques must be set up just as the use of security technology. It helps to ensure e-Government systems against attack, recognizes great exercises administrations and to have a demonstrated alternate course of action set up. An open private organization is a vital part of cybersecurity in E- Governance. These associations can conveniently go up against coordination issues. Powerful cyber-crime prevention and arraignment activities in all the ICT appropriate conditions.

2.1.2 Kaspersky Kidnapping Case [3]

The "highest-profile" cyber surveillance, stalking, and kidnapping case included Ivan Kaspersky, child of the administrator and CEO of Russia-based Kaspersky Lab, a standout amongst the most unmistakable cybersecurity firms on the planet. Ivan Kaspersky was abducted for payoff in 2011 while strolling to work from his Moscow loft. As indicated by Russian media sources, beginners – a more seasoned obligated couple – organized the plot and enrolled their child and two of his companions as "muscle" for the plot (Cabaj, Kotulski, Księżopolski, & Mazurczyk, 2018). The abductors stalked Kaspersky and his sweetheart for a while preceding the seizing, deciding his conduct standards and finding that he did not have a protective security detail. The hijackers supposedly acquired all the required data from Kaspersky's client profile on Vkontakte, a famous Russian social systems administration site. Kaspersky was compelled to call his dad to transfer the payoff requests (Gade, & Reddy, 2014). The abductors may have utilized similar wireless to make food deliveries or had geolocation administrations empowered.

2.1.3 Uber Case study [4]

Data breaches happen every day, in too many places, but the risk of data breach doesn't necessarily depend on the number, it may also depend on the risk and damage it causes the company's revenue and impact on the users or account holders, one of the biggest recent data breaches is Uber.

[A] Impact:

One of the recent major cyber-attack [5] is data breach of personal information of around 57million Uber users and 600,000 Uber drivers got revealed.

[B] Details:

The worst part of this attack [6] is how the Uber handled the issue, this is a lesson to most companies what not to do. In late 2016 just two hackers were able to steel the Users personal data with includes names, phone numbers and email addresses. They were able to steal the 600,000 driver's license information. Hackers got access to the Uber's GitHub account through a third-party cloud- based service. With the details found from the GitHub, Hackers found a way to access Uber user data in AWS. Ubers paid those two hackers $100, 000 to permanently destroy the whole data they obtained and not letting the users or the regulators about stolen information.

But also, Uber confirmed that data was destroyed with the assurance they received from the hackers. According to US Law enforcement, any breach should be reported to the authorities and not pay hackers. And this kind of approach from Uber led other hackers to blackmail Netflix, where Hackers frightened to release TV shows unless the company paid the money hackers requested. Almost 49 states have this law enforcement where a security breach should be notified, after the court hearings Uber agreed to pay 20million to settle FTC charges. Not only the US but also other major countries like UK, Italy, and the Philippines reacted on this issue. Uber's breach is different from the regular breaches, the company tried to cover up the breach and not alert the authorities and the users.

[C] Uber's plan after the breach:

Khrosrowshabi the new CEO of Uber received few disputed problems only with respect to its legal issue also criticism for sexual harassment, underpaying the drivers and few more.

Solutions:

1. Access control and “password security”.

2. Data’s Authentication.

3. Anti-virus Software.

4. Malware Scanners.

5. Firewall.

Chapter 3

Categories of Cyber Crime

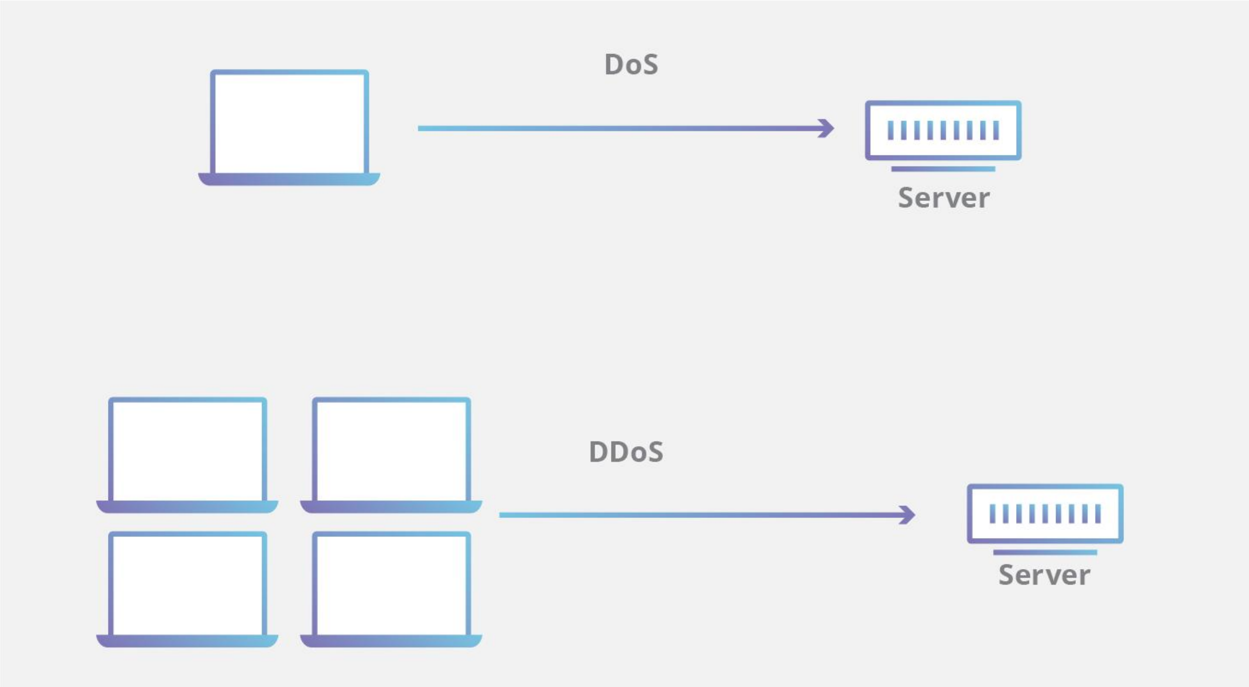
- **Hacking**
- **Denial of service attack**
- **Virus Dissemination**
- **Computer Vandalism**
- **Cyber Terrorism**
- **Software Piracy**

Hacking

- Hacking in simple terms means an illegal intrusion into a computer system and/or network.

Denial of service attack

- Act by the criminal, who floods the bandwidth of the victim's network.
- Is his e-mail box with spam mail depriving him of the services.



Virus Dissemination

- Virus dissemination is a process of a malicious software that attaches to other software that destroys the system of the victim. They disrupt the computer operation and affect the data store by modifying or deleting it.
- Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, web jacking, e-mail bombing etc.)

Computer Vandalism

- Damaging or destroying data rather than stealing.
- Transmitting virus

Cyber Terrorism

- Use of Internet based attacks in terrorist activities.
- Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

Software Piracy

- Theft of software through the illegal copying of genuine programs.
- Distribution of products intended to pass for the original.

Chapter 4

Prevention and Security

You might think that the only form of cybercrime you have to worry about is hackers stealing your financial information. But it may not be so simple. There are far more concerns than just basic financial ones. Cybercrime continues to evolve, with new threats surfacing every year.

When you hear and read about the range of cybercrimes out there, you might be tempted to stop using the internet entirely. That’s probably too drastic.

Instead, it’s a good idea to know how to recognize cybercrime, which can be the first step to helping protect yourself and your data. Taking some basic precautions and knowing who to contact when you see others engaged in criminal activities online are also important steps.

- Use antivirus software's.
- Insert firewalls.
- Uninstall unnecessary software
- Maintain backup.
- Check security settings.
- Use strong passwords
- Keep your software updated
- Manage your social media settings
- Stay anonymous - choose a genderless screen name.
- Never give your full name or address to strangers.
- Learn more about Internet privacy.

Chapter 5

Conclusion

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe.

The “cyber-terrorism” can in one method or alternate prompts the death toll just as causing severe harms and massive loss of money to the organization. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. Cyber terrorism has guaranteed numerous innocent lives and in the meantime render numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. Cyber terrorism stays vital issues of the present society. Not just that the battle against Cyber terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational. Cybersecurity has an intriguing parallel to terrorism. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a system.

Chapter 6

References

[1] Mrs. Ashwini Sheth1, Mr. Sachin Bhosale2, Mr. Farish Kurupkar3Asst. Prof.1, Department of C.S., I.C.S. College, Khed, Ratnagiri H.O.D.2, Department of I.T., I.C.S. College, Khed, Ratnagiri Student3, M.Sc. I.T., I.C.S. College, Khed, Ratnagri CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE : APRIL, 2021 RESEARCH PAPER ON CYBER SECURITY

[2] https://www.irjet.net/archives/V2/i8/IRJET-V2I846.pdf

[3] https://worldview.stratfor.com/article/kaspersky-kidnapping-lessons-learned

[4] https://www.corporatecomplianceinsights.com/responsibilities-consequences-uber-data-breaches/

[5] https://www.mondaq.com/turkey/data-protection/768680/a-case-study-in-data-breaches--uber39s-data-security-breach-fines-reach-usd-150-million

[6] https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users

[7] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/after-uber-data-breach-lessons-for-all-of-us.html