CYBERSECURITY AND CYBER ATTACK

Rakshit Kapoor[1], Kuldeep[2], Rohan Shokeen[3]

[1]*Enrolment No 01914004421*
[2]*Enrolment No 02114004421*
[3]*Enrolment No 02314004421*

ABSTRACT

With the advancing time, the world is getting advanced and digital. And with this advancement comes the risk of attackers. This is why cyberspace needs security. The term used for this term is ***CYBERSECURITY****. With the advancing world, especially during this time of thepandemic, nearly every work is done online. The internet is filled with valuable data starting from somebody's personal information to even their bank account. The attackers try to steal these data for personal or professional gain. There are plenty of ways of attacking any system for instance the most popular and used way of attacking,* ***MALWARE****. It is software that is solely developed to damage and destroy a computer system in other words it is "malicious software". This malware is developed to tackle every known defense mechanism resulting in the desperate need for the continued improvement in the defense mechanism. This paper intends to give little understandingof the need for cybersecurity. [i]*

KEYWORDS: *Cyber security, Cyber-attacks, Security Techniques, Prevention*

I. INTRODUCTION

Our world today is greatly dependent on technology. Cyber-attacks have become pretty common and as much disastrous due to the dependence on technology. Due to the pandemic, the transition from physical to digital workbench has resulted in a dramatic increase in both criminal attacks as well as ransom attacks. According to the research, India was the most affected country in the world. All the countries across the globe are increasing the budget sanctioned to the cybersecurity sector due to the recent increase. Today, the world is getting more aware of the vulnerability that has developed due to the increase in dependence on technology. The attackers are getting more and more advanced along with the technology, we also need to step up to protect our data as much as we could. One of the main questions that arise due to the recent events is, **Why has cybercrime starting to surface?** The reason is simple. Committing cybercrime is less risky and cheaper when compared to physical attacks. The need for **CYBERSECURITY** has never been higher. [iii]World Wide web (WWW) was created in 1990s by Sir Tim Berners, after which began the demand for public access of it due to its ease of solving many problems. But with every great thingcomes the worst part of it as well, Cybercrimes. Cybercrimes have many forms like cyberbullying, Identity theft, Phising and many more. But most of it is commited by the unethical hackers for some personal or professional gains. The amount of harm that these tactics may cause is unfathomable. One can virtually assume anyone's identity and access from personal data to professional which can eventually end up affecting victim's life in a bad way. There are countless cases of cyberbullying resulting in victim developing depression as well so these attacks are far worse than physical attacks as it affects a person's mental health. [iv] Cyberattacks are getting more and more deadly with the evolving world. With passing time worldis getting bent towards the technology making the world more and more exposed towards the danger of getting attacked virtually. For example, the **TESLA** car that is capable of driving itself on its own or now-a-days a lot of house assistants are developed with smart artificial intelligence like alexa or google home. Every mobile device already has adapted some sort of AI to ease its work like apple uses SIRI and android Google. These adaptions does ease our works but also makes it vulnerable to attacks which is why the manufacturers already spend a hefty amount of their budget in order to make them as secure as possible. But still there are always some who come up with some sort of algorithm turning it into codes and eventually a software which is popular as **MALWARE**. These malwares are made with the target in mind and have the capability to harm the same. Then there comes **PHISHING,** a reputed and trusted name is used to send a malicious link of some sort via message or emails, upon clicking it makes the system vulnerable and could be used to steal sensetive data. There are also methods of hacking a website if it seems impenetrable from outside, like finding the server one is using and then attack some other website which happensto be less secure and operates on the same server and through that reaching the target gets easier. [v]

Whatever is done the attackers would always find their ways in. So, What's the answer to this dilemma? **Evolution in cybersecurity** is the only current solution and may would be only solution.

II. STUDY OF CYBERSECURITY AND CYBER ATTACKS

Cybersecurity is often mistaken as a way to protect themselves from hackers only, but this is only a part of the complete picture. Cybersecurity is not a term that indicates making one's devicecompletely impenetrable but its more like an insurance that it won't be harmed that easily. In todays world every organisations be it government or private use computer networks and the technologiesand this has resulted in the security with utmost importance. And now cybersecurity is being moreimportant with the passing time since everything be it car or metro, a house or even an entire city is becoming smart by adapting technologies to operate themselves. With the growing world, we are able to operate everything from lightbulb in our room to our vehicles with nothing but a digitalnetwork connected to our device. **What is the definition of smart city?** A city which uses everything starting from AI to colud computing and what not. In short, a smart cities are vast systems that are closely interdependent. But can we truly call any city so heavily reliant on technology a smart city? It won't be much of a smart city if it is that easy to damage. We can deducethat transitioning a city from connected to smart is complex and time-consuming as it involves a high level of reliance and connectivity across its levels, it is a security-conscious procedure. This section covers the most serious security concerns and violations that might ariseat any stage of a city's smartening.

Cyber-physical infrastructure utilised in city smartening has a number of weaknesses andhazards. Despite the widespread usage of modern cyber-physical infrastructure systems, there is no satisfactory understanding of their vulnerabilities and dangers. We'll go through the most common infrastructure security risks and problems.

- **Cameras:** Cities are littered with private and public cameras, all of which are secured in various ways by encryption and username/password security. Accessing private or publiccameras and having access to them violates people's privacy while also spying on government interests.
- **Building Management Systems:** Designers and developers of such systems typically focus on the service offered while ignoring cyber security concerns. As a result, manufacturers of such systems do not provide notification options for users to be notifiedabout security violations.
- **Eavesdropping:** Install eavesdropping tools on a network segment to monitor communication channels, record network behaviours, and generate a network map. Itcan result into a huge personal or professional loss.
- **Theft:** It has an impact on urban infrastructure by stealing both intangible items like sensitive data, information, credentials, software, and cryptographic keys, but alsogadgets and technical equipment. It compromises the availability and confidentiality of systems, resulting in financial losses and a tarnished image.
- **Denial of Services DoS:** This process is to overburden connections until services andgadgets that rely on them become unavailable. Attacks on systems or connections via denial of service (DoS) have a negative impact on their availability.
- Other dangers include device failure, software crashes, environmental and natural behaviors, and vendor and manufacturer support termination. Such attacks compromise the availability and integrity of infrastructure systems, resulting in production and servicedelivery failures.

Smart Cities deal with massive amounts of real-time data and associated data-driven technologies that act on, create, analyse, execute, and produce data. Many resources in smart cities produce many sorts of data.

III. CYBER SECURITY TECHNIQUES

1. Strong Password Security: Increasing the security of your system is made simple by usinga strong, complex password. For instance, a password with letters, numbers, and special characters It can be prevented from being cracked by brute force by routine update.
2. Authentication of knowledge: Regular updates and use with prudence are important for knowledge authentication since hackers and programmers can take advantage of email andthe web in many different ways. System updates and routine backups are fantastic ways topreserve your data, ensure that it can be retrieved, and fix any faults or flaws in the system.

3. Malware scanners: Programs that examine all files on the device for malicious code and viruses. Malicious software is referred to as malware and includes worms, Trojan horses,and viruses as examples.
4. Firewalls are pieces of hardware or software that help identify hackers, viruses, and worms that try to access your device through the internet. Every message entering orleaving the web is examined by the firewall, which prevents any that don't meet the minimum security requirements.

IV. CASE STUDY ON CYBER ATTACKS

i. Andhra Pradesh Tax Case [iv]

In Andhra Pradesh, the owner of a plastic company was taken into custody. Twenty-two crores incash were retrieved by the Vigilance Department from his residence. They demanded information and explanation from the individual regarding the undeclared money. 6,000 vouchers were deposited by the defendant to confirm the legitimacy of the company. But it turned out that all of the vouchers were created after the raids were carried out after a careful review of the data and vouchers on his PCs. In order to present sales records and avoid paying taxes, it was discovered that five enterprises were operating in the same space as a single company. As the department authorities seized the accused's computers, the Andhra Pradesh chief businessman's interrogation techniques became apparent.

ii. The Bank NSP Case [v]

The Bank NSP case involved a bank management trainee who was both engaged and getting married. The couple utilised the business's PC and sent and received numerous emails and messages. The young lady created false email accounts with the name "Indian Bar Associations"and sent emails to the man's international clients when the two eventually split up. She completed this on the bank's computer. The man's business lost a lot of clients, and it sued the bank in court to recover those losses. The emails sent via the bank's system or PC belonged to the bank, and the bank was accountable for them.

iii. State of Tamil Nadu vs. SuhasKatti [vi]

This case is related to the publishing of an offensive, hurtful, and graphic message about a divorced woman in a Yahoo texting group. Additionally, emails were sent to the victim seeking proof by the suspect through an incorrect email account he opened in the victim's name. Due to the lady's posting of the message, she received bothersome calls from people who mistakenly thought she was soliciting. In response to a report the victim filed in February 2004, the police tracked the suspect down to Mumbai and apprehended him within a short period of time. The offender was apparently interested in marrying the victim since he was a well-known family friend of hers. She married someone else, though. The accused began contacting her again after this marriage ended in divorce. The accused began harassing her online because to her hesitationto marry him. Twelve witnesses were questioned by the prosecution, and complete papers were designated as exhibits. The court determined that the offence was conclusively proven and foundthe accused guilty based on the expert witnesses and other evidence presented to it, including witnesses for the owners of the Cyber Cafe. This is thought to be the first instance in Tamil Naduwhere the criminal was found guilty under section 67 of the Indian IT Act.

iv. Online Credit Card Fraud on e-Bay [vii]

Police in Rourkela break a scam that included a $12.5 million online fraud. The accused's "modus operandi" was to hack into the eBay India website and make purchases using other people's credit cards. Two people—including the BCA student suspected of being the plot's mastermind, Debasis Pandit— were apprehended and brought before the Rourkela court of the subdistrict judicial magistrate. Rabi Narayan Sahu is the other person who has been taken prisoner. Under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act, a case has been filed against the accused. Approximately 700 credit cardholders' personal information was allegedly collected by DebasisPandit after hacking into the eBay India website.At that time, he used their passwords to make purchases. When it was discovered that just a small number of purchases were made from Rourkela while the clients were located in locationslike Bangalore, Baroda, Jaipur, and even London, the fraud was brought to the attention of eBayofficials. After some customers complained, the business brought the problem to Rourkela police's attention.

V. CYBER ETHICS AND PRACTICES FOR PREVENTION OF CYBER ATTACK

1. Do communicate and engage with others online. Keeping in touch with family, friends, and coworkers is made easier through email and texting. sharing fresh ideas, knowledge, and understanding with others locally or globally.

2. Never exchange or transfer personal information over an unencrypted network, including unencrypted mail, such as your bank account number, password, ATM pin, and so forth.
3. Never join up for a social networking site or platform until you are sure that it is legitimate andreal.
4. Never neglect to update and renew the operating system. One should install and regularlyupdate software like firewalls, anti-virus, and anti-spyware programmes on their PCs.
5. Never go to, follow, or respond to a spam website or link.
6. Avoid being a bully or a harasser online. Avoid using insulting words or phrases. Don't insult individuals, call them names, send them obscene or embarrassing photographs, or try to injurethem.
7. The internet is regarded as the world's largest library, offering data on every subject and field of study. Therefore, use this information ethically and legally.
8. Never divulge your password to anyone, and never use someone else's password to accessyour account.
9. Never give out your personal information to anyone since there is a chance that someone elsewill misuse it and you will be held responsible.

CONCLUSION

So atleast in every organisations be it government or private or even NGOs that uses computer network must give their employees atleast the basic knowledge of cybersecurity to prevent any tragedy from happening. Cyber security in smart cities is a critical problem that requires consideration of a number of security risks related to technology, applications, infrastructure, and data. The growing integration of technologies, as well as the resulting intensive communication, high complexity, and high interdependency, has a significant impact on cyber security, resulting in an unbounded attack surface and cryptography-related difficulties. Smart city cyber security is a critical issue that necessitates worldwide collaboration with specialists from all around the world. India, a nation of 1.3 billion, has the lowest data rates worldwide. The advancement of the network has increased the importance of data and information security. This study makes it quiteevident that as cyberspace and technology advance, so will the range of cyberthreats. To protect data, one must take precautions such as installing antivirus software, employing firewalls, creating strong passwords, and practising hacker avoidance. India needs to switch from its current reactive strategy of merely protecting its cyber system when cyber security incidents occur to a proactive one. Because it is very necessary. To sustain the rule of law, awareness campaigns, firm modifications, criminal laws, and cyber security regulations are required to defend rights and privacy.

REFERENCES

1. *Aldairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science, 109(2016), 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391*
2. *Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005*
3. *Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cybersecurity attacks to modern vehicular systems. Journal of Information Security and Applications, 36(October), 90– 100. https://doi.org/10.1016/j.jisa.2017.08.005*
4. *https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware*
5. *RESEARCH PAPER ON CYBER SECURITY Mrs. Ashwini Sheth1 , Mr. Sachin Bhosale2 , Mr. Farish Kurupkar3 https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security*
6. *Indian Cyber Security Andhara Pradesh Tax Case*
7. *https://www.indiancybersecurity.com/case_study_andhra_pradesh_tax_case.php#:~:text=Dubi ous%20tactics%20of%20a%20prominent,sleuths%20of%20the%20Vigilance%20Department.*
8. *Indian Cyber Security The bank nsp case https://www.indiancybersecurity.com/case_study_the_bank_nsp_case.php*
9. *Indian Cyber Security State of Tamil Nadu vs.SuhasKatti https://www.indiancybersecurity.com/case_study_state_of_tamil_nadu_%20suhas_katti. php*
10. *https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html*