International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Poly Mechanisms, Technology and Challenges in AI and Cyber Security

T.C.Sujitha

Assistant Professor, Department of Computer Science, Mannar Thirumalai Naicker College, Madurai, Tamilnadu, India

ABSTRACT: Cyber security plays an eminent role in Digital Era. It secures individual and organization information from the harmful hack in the present Era. It can protect information systems and networks. Due to Immensely increasing cyber crimes, we have to protect our data from the transformation. A Cyber criminal focuses on social media websites and Net banking. Some of the recent attacks of cyber crime in India have discussed. This paper mainly focuses on challenges faced by cyber security on the latest technologies like AI, Cloud computing, smart phones and Internet of things. It center points on the latest about protection techniques, ethics and challenges the cyber security.

KEYWORDS*:* AI, Attacks, Cyber crime, Social media

I. CYBER SECURITY

Cyber security deals with digital era risks, transformation vulnerabilities and improving system flexibility. Cyber security is an important tool in protecting and preventing the data from the unauthorized crackers. ICT plays an important role nowadays among the dawn of the internet, security becomes a major concern. ICT devices are connecting with the IoT and secure the data. We can secure the information through act of protecting ICT systems are known as cyber security. Computer Security protects the system based on the following technologies like Hardware Authentication, User Behavior analytics, Data Loss Prevention, Deep Learning, The Cloud. We can categorize the security as application security, Information security, network security, web security, mobile security and operational security.

a) Application Security
b) Information Security
c) Network Security
d) Web Security
e) Mobile Security
f) Operational Security

II. TYPES OF ATTACKS

Security is the main thing when we have network connection. The hackers are countless. They are searching new ideas and use the old attacks to theft the information. To protect a computer system, we must know the attacks that can be made against it. We will see some of the attacks which play a major role in nowadays.

Direct Access attack – The, hacker includes a privilege as physical access to steal and gaining the information.

Indirect Access attack – The system won't permit means, hacker choose some trusted system through the system unauthorized person access the information.

Eavesdropping - Without knowing the person copying and send to the some harmful person or organization.

Spoofing – Employing a program or by person creating a false record through that get the information. We will say our email too.

Phishing – It's a method to require the end user data using ATM cards through the Network connection. Login credentials, master card numbers, and passwords are usually what such hackers obtain from their victims.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Cyber Espionage - Cyber espionage is an international problem in today's world. We don't seem to be conversant in this term, but we well understand about this attack ie Confidential data which is kept by the Trusted Places of Government sector, Military, Organization or individual data without knowing their aware, hackers steal the records use of some malicious software, proxy servers. Ex: Bluewhale game

Botnet - Botnet is a group of computers that takes control of each internet-connected devices to carry out distributed denial of service (DDOS) attack, send spam and hackers to sabotage the connection and devices.

AI-Powered attacks – Nowadays AI roles in our part of the life. Many AI related cars, computer systems are hacked by hackers which leads to the security problems in national level too. Example: Monitoring the patient and suspicious system or malfunctioning system gives the report in negative.

Types of attacks reported due to COVID 19 are Denial of Services, Cyber Attack, and Physical assault. Phishing attacks took major place in payment, web mail, financial institutions, Social media, cloud storage, retail and telecom.

III. TECHNOLOGY FOR CYBER SECURITY

1) Cryptographic systems: The encrypted data and cipher text of the code use to transform the information.
2) Firewall: Use to block traffic from outside, but it could be also used to block traffic from inside.
3) An Intrusion Detection System (IDS): IDS is an additional protection measure used to detect attack.
4) AntiMalware Software and scanners: Autorun Viruses, worms, bombs and Trojan horses are all examples of malicious software, or Malware for short. We can use antimalware software to detect suspicious files in our drives
5) Secure Socket Layer (SSL): It is a suite of protocols that is a standard way to achieve a good level of security between web browser and websites.

IV. INCREASE IN CYBER ATTACKS IN INDIA 2020

India has affected by the cyberattacks by 37%. This attacks were happened by online and offline modes. In online based on our login credentials, ATM/ Credit cards, unknowingly installed the application from devices. In offline the malware spread by USB drive, SD cards, CD's and DVD's. The solution for the attacks is protection of our data from the antivirus, anti-rootkit, firewall and proxy servers.

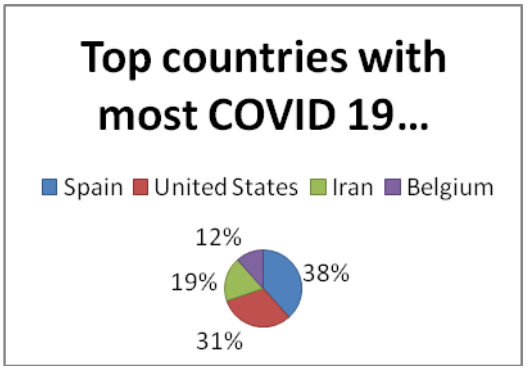
|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India



V. ARTIFICIAL INTELLIGENCE

Artificial intelligence is frequently portraying scholarly capacities that machines connect with the human brain. Artificial intelligence occasionally called machine intelligence; investigation associated with artificial intelligence is highly technological and expert. Is AI assumes a significant job in digital security? Truly. There was many exploration papers are demonstrating this. These days AI become as blast and boycott in digital security.

Artificial intelligence is ending up being a help for cybercriminals as well. Consider it – the AI capacities used to distinguish and stop cyberattacks can likewise be utilized by programmers to dispatch refined cyberattacks as intricate and versatile vindictive programming.

AI fuzzing (AIF) and machine learning (ML) poisoning are good to go to be the following enormous cybersecurity dangers.
AI fuzzing integrates AI with traditional fuzzing techniques to create a tool that detects system vulnerabilities. AI fuzzing can assist enterprises detect and fix the vulnerable activities in their system, it can also be used by cybercriminals to start, automate, and accelerate zero-day attacks.
Machine Learning Poisoning If a hacker targets a machine learning model and injects instructions into it, the system becomes vulnerable to attacks. Machine learning models typically use data that is crowd-sourced or taken from social media.

VI. AI APPLICATIONS ARE USED IN CYBER SECURITY

Following application categories can be examined on AI in cyber security

- Spam Filter Applications (spamassassin)
- Network Intrusion Detection and Prevention
- Fraud detection
- Credit scoring and next-best offers
- Botnet Detection
- Secure User Authentication
- Cyber security Ratings
- Hacking Incident Forecasting

VII. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Web-based media are online correspondences that permit people to making and sharing of data by means of virtual networks and systems. They can share sound, video, text and a lot more over the Internet. Life turns out to be extremely simple as opposed to past times.

Today everywhere on over the world existence of people groups are encircled by web-based media and Internet. They need online media and Internet in their staff life. To escape from the cyberattacks we need digital security. List of Cyber Crimes under an IT Act:

- Hacking with computer systems

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- Publishing obscene information
- Unauthorized access to protected system
- Bogus websites, cyber frauds
- Email spoofing
- Social websites hacking
- Email abuse
- Misuse of social media.

VIII. SOCIAL MEDIA POLICY AND SECURITY

In this pandemic time, we are investing our energy in web-based media. Be that as it may, each online media have the arrangements and security. The organization has the duties about the classified data.

The unmistakable data ought to be given to the workers, what are the necessities by them to help protect data that ought to be start from screen locks to the ideal secret key changes.

Company ought to clarify all the security settings to the workers who are generally joining as preparing individuals. · All the representatives should think about any outer or inner assaults on the organization private information or data web-based media.

The ordinary instructional courses ought to be given to the workers for security and protection of organization information or data.

IX. CYBER ETHICS

Cyber ethics is an ethics which gives about the information of computer system, What & How computer programmed to do, and it affects the individual and organization. It will give innovative ideas, when we make a practice that how to use the Internet in proper way. We should take care of the children and teenage people how to use the Internet with the security. Here Some Pro's and Con's of the below are a few of them:

- We use the Internet to communicate with our fellow people. We can use various applications like gmail, whatsapp, Hike and instant messaging make us easy to stay in touch with our buddies and family members, communicate with work colleagues, and sharing our ideas and thoughts around the world to our known persons.
- Don't be a bully on the Internet. Do not share suspicious pictures and memes without acknowledge the truth.
- World Wide Web (WWW) term is known by everyone even though children because of online classes. We can search anything related to our subject, Health oriented.
- Do not try others email accounts using their passwords.
- Today's government follow everyone, so don't forward malware to anyone.
- Well know fact! Don't share your information, OTP, CVV numbers to others, it leads to a big mess to you.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Make sure you are stick on the policies and copyrights whenever install the new software or app.
- Don't install third party application (app) which steal your information and malfunctioning with our information.
- Every parent should enable the Parental control in the playstore settings when the child is trying to install an unknown application. This makes the children without knowing parent couldn't install other application.

The above few are some Pro's and Con's about the cyber ethics. The person who uses the Internet should aware of this.

X. CONCLUSION

Cybercrime influences the people and impact of the crime that leads to the individual to end of the life sometimes. We must care about our websites and application cookies, which contains malware too. In case of cyberbulling, we must take necessary actions and never respond to the messages. Every company must have a security related software and policies. We can secure our data use a VPN, encrypt our mail, careful with links, passwords to be aware of public Wi-fi and use anti-malware or anti-virus protection.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

REFERENCES

[1] https://www.ubs.com/microsites/artificial-intelligence/en/new-dawn.html
[2] https://dst.gov.in/basic-research-cyber-security
[3] https://ieeexplore.ieee.org/abstract/document/8819719
[4] https://ieeeaccess.ieee.org/special-sections-closed/artificial-intelligence-in-cybersecurity/
[5] https://www.business2community.com/cybersecurity/10-ways-to-keep-your-information-safe-in-the-digital-age-02130163
[6] https://www.easychair.org/cfp/cybersecurity2019
[7] https://cio.economictimes.indiatimes.com/news/digital-security/top-cyber-security-trends-that-will-shape-2020/73119945
[8] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
[9] https://blog.rsisecurity.com/what-are-the-different-types-of-it-security/
[10] https://theknowledgereview.com/cyber-ethics
[11] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
[12] Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[13] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[14] https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field
[15] G. Nikhita Reddy, G. J. Ugander Reddy (2014)."A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES"
[16] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v.5508. Springer, 2009, 279-286 [17] https://eezytutorials.com/Cryptography-And-Network-Security/Security-services-and-mechanisms.php#.X1S-_SgzZdg
[17] https://www.academia.edu/25349174/ARTIFICIAL_INTELLIGENCE_IN_CYBER_SECURITY
[18] https://ieeexplore.ieee.org/document/8601235
[19] http://paper.ijcsns.org/07_book/202002/20200216.pdf