**International Journal of Advanced Research and Development**
**www.advancedjournal.com**
**ISSN: 2455-4030**
**Received: 21-12-2021, Accepted: 05-01-2022, Published: 21-01-2022**
**Volume 7, Issue 1, 2022, Page No. 4-6**

# Cyber security: Study on attack, threat, vulnerability and prospective solutions

**Ikhlas Ahmad Sheikh[1], Firdoos Ahmad Wani[2]**
[1] Lecture, Department of Computer Application, Government College for womens Srinagar, Jammu and Kashmir, India
[2] KISD (Kashmir Institute of Skill Development), Jammu and Kashmir, India

**Abstract**
The main objective of this research work is cyber security, threat, attack and vulnerability of cloud infrastructure and how these cyber attacks occur. It also discusses the perspective solution in order to prevent from these attacks and threats. This paper also discusses the cyber security and its role to secure from these vulnerabilities. It also discusses the various cyber attacks that have been done. This paper concludes that the technology had played an important role in reducing the impact of these attacks, threats and vulnerabilities.

**Keywords:** cyber security, malware, threats, attacks, vulnerability, Trojans

## Introduction
The Internet have changed the world with the new technologies in many ways but at the same time opened the doors of so many challenges that have seen never before. Today's world is advanced and is going into the digitalization or cash less transaction. Every organization either government, private or other have accomplished significant cyber loss. As fast as security heightens, the hacking world grows faster. During this period people are accessing social media platforms such as Facebook, Instagram, and whatsapp. In addition to this most of the people watch movies and shows by subscribing to web channels like Hotstar, Amazon, Jiotv etc. and giving permission to access their personal information in order to use their services. All these activities have opened the door for spyware and ransom ware attacks. Cyber security involves protecting the information by preventing, detecting and responding to cyber-attacks [1].

## What is cyber security?
Cyber security is the implementation of technologies, processes and controls to protect or secure systems, networks, programs, software's, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and secure against the unauthorized misuse of systems, networks and technologies.
Cyber security is the execution of protecting critical systems and sensitive and careful information from digital attacks. Cyber security also known as information technology (IT) security, cyber security measures are designed to tackle threats against networked systems and applications.

## Background
In this internet world cyber security is an important topic to discuss due to the reason that number of attacks have been done on government sector, organizations, banking sector etc. In recent studies number of attacks like cyber war has been done. Cyber security is a hot issue to debate that can motivate many independent scholars, experts and researchers to think about the topic and give best solutions to these cyber attacks.

As per the cyber crime data maintained by the National Crime Records Bureau (NCRB), a total of 217, 288, 420 and 966 Cyber Crime cases were registered under the Information Technology Act, 2000 during 2007, 2008, 2009 and 2010 respectively [2].
Indian Computer Emergency Response Team (CERT-In) issues alerts, advisories and guidelines regarding cyber security threats and measures to be taken to prevent cyber incidents and enhance security of Information Technology systems.
Akamai Technologies' State of the Internet report also showed that hacker attacks on websites went up 75% in the final quarter of 2013, with hackers in China responsible for 43% of all attacks [9].
Risk Based Security reports the highest number at 6,515 breaches and 5 billion exposed records, both down from 2017 [10].

## Methodology
Proposed method works to give more importance to cyber attacks, threats and vulnerability and also describe some solutions to prevent these cyber attacks. We try to highlight some important developments and look to future trends. The range of operations of cyber security involves protecting and securing information and systems from major cyber attacks. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people.

## Threats
Cyber security threat is a malicious activity by an individual or an organization to gain an unauthorized access to other individuals or organizations data or information.
A cyber threat or cyber security threat is a malicious act intended to steal or damage data or disrupt the digital wellbeing and stability of an enterprise. There is crimes that target computer networks or services directly like malware, viruses or denial of service attack and crimes facilitated by networks or devices.

**Types of Threats**

**Malware:** Short form malicious software which is specially designed to disrupt damage or gain unauthorized access to a computer system. They are self replicating and spread very fast. There are various types of malwares-

**a. Virus-** A malware which requires some form of user interaction to infect the user's device. Example is email-attachment.

**b. Worm-** A malware which can enter a device without any explicit user interaction. It can contain logic bombs.

**c. Logic bomb-** A logic bomb is a piece of code intestinally inserted into software that will set off a malicious function when specific condition is meant.

**d. Trojan-** Trojan horse is any malware which misleads user of its true intent. They are programmed that claim to perform one function but actually do another.

**e. Spyware-** Spyware is software that aims to gather information about a person or an organization, sometimes without their knowledge, they may send such information to another entity without the consumer consent.

**f. Denial of service-** An attacker sits between the sender and receiver and capture the information then retransmit to the receiver after sometime with or without altering the information.

**Possible solutions to prevent from Threats**

a. Keep computer and software's updated.
b. Be careful before opening an email attachment.
c. Always make secure connection (HTTPs).
d. Use firewalls, antimalware etc.
e. Install antivirus software.
f. Do not click on specious links from unknown source.
g. Backup your data.
h. Signature based malware detection mainly used by antivirus whereby scanner scans for a sequence of byte within a program code to detect and report malicious code. Malware detection using this approach involves a syntactic level of code instruction by analyzing the code during program compilation [4].

**Attacks**

A cyber-attack is when someone gain or attempts to gain unauthorized access to a computer maliciously [3]. Cyber attacks are very critical issue that needs to be discussed and aware people about these attacks. A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

**Types of cyber Attacks**

**a. Phishing-** Phishing is the method of sending fraudulent communications that seems to come from a reputable source, usually through email. The goal is to steal or get sensitive data like credit card and login information or to install malware on the victim's machine.

**b. Man-in-Middle-** This attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. It is also called eavesdropping attacks.

**c. IP-Spoofing-**The ability to inject a packet into the internet with a false IP address. IP spoofing involves modifying the packet header with a spoofed source address, a checksum and the other values.

**d. SQL-Injection-** A Structured Query Language (SQL) injection happens when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

**Possible solutions for cyber attacks**

a. End to End authentication for IP Spoofing.
b. USE Multi-Factor Authentication- One of the most effective ways to prevent cyber attacks is to ensure that multi-factor authentication has been enabled for all applications that access the internet in an organization. [5].
c. CREATE Robust Internal Controls- To prevent cyber attacks in an organization it's also crucial that there are robust internal controls in place. Access controls will help ensure that system access is updated immediately once employees, contractors, and vendors leave the organization [5].
d. Pre-Deployment & Post-Deployment Technique (Tautology attack) [6].
e. Static Pattern Matching Algorithm (Stored Procedures) [7].
f. Always be suspicious of password reset emails.
g. Never share your crenditals.
h. Shopping safely online

**Vulnerability**

In cyber security, vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting vulnerability, a cyber attack can run malicious code, install malware and even steal sensitive data.

Many security authorities have defined vulnerability as:

- **National Institute of Standards and Technology (NIST):** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- **ISO 27005:** A weakness of an asset or group of assets that can be exploited by one or more cyber threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission [8].
- **IETF RFC 4949:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

**Common types of cyber security vulnerabilities**

- Out dated software
- System misconfigurations
- Poor data encryption
- Poor password management
- Zero day vulnerability

**Possible solutions for cyber security Vulnerabilities**

- Use updated software's
- Strong passwords- use numbers, alphabets and special characters.
- Install firewalls

- Data back and recovery
- Educate people about these security threats
- Safe browsing

**Conclusion**

Hence in a nutshell, with the rapid growth on malware, attacks and threats proactive approaches must be undertaken to secure network computing environment. Cyber security incidents involving attacks, research supports the most effective defense is a computer literate user. This paper concludes that while technology has a role to play in reducing the impact of cyber-attacks, threat and vulnerability resides with human behavior, human impulses and psychological predispositions that can be influenced through education. Cyber-attacks can be reduced, but an absolute solution to overcome such cyber security threats has yet to be put-forward. So further research is needed in order get the better solution for securing from these malwares, Vulnerability and threat.

**References**

1. Razzaq, Abdul, *et al*. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. “Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.
2. Available on: Indian cyber security http://www.indiancybersecurity.com/cyber_crime_on_the_rise.php
3. “Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users” International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2015, 9:3.
4. Surajudeen A, Mabayoje M, Mishra A, Oluwafemi O. Malware Detection, Supportive Software Agents and Its Classification Schemes. International Journal of Network Security & Its Applications (IJNSA), [online],2012:4(6). Available at: https://www.idc-online.com/technical_references/pdfs/data_communications/Malware%20Detection.
5. Cyber attack-what you need to know Available at- https://www.unisys.com/glossary/cyber- attack/
6. “Runtime monitors for Tautology based SQL Injection attacks”, Ramya Dharam, Sajjan G.Shiva, “International Journal of Cyber Security and Digital Forensics (IJCSDF) I(3):189-203 The Society of Digital Information and Wireless Communication (SDIWC) 2012 (ISSN: 2305-0012)
7. “Detection and Prevention Of Sql Injection Attacks Using Novel Method In Web Applications”, Tejinderdeep Singh Kalsi, Navjot Kaur, Int J Adv Engg Tech/Vol. VI/Issue IV/Oct.-Dec.,2015/11-15, E-ISSN 0976-3945
8. Available at- vulnerability definitions- https://www.upguard.com/blog/vulnerability
9. Brutal Cyber Attacks- https://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5- most-brutal-cyber-attacks-of-2014-so-far/?sh=462d41ee134d
10. Internet Society- https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report