Security in Internet Web Systems

Sravani Dhanekula - 02043337

Abstract: - Security and privacy in web systems have become paramount concerns in today's digital age. With the increasing use of the Internet for various activities, such as online purchases, communication, and networking, individuals expect their data and communications to be kept private and confidential. In this paper, we delve into the multifaceted realm of web and networking security and highlight the vulnerabilities within these systems. The discussion encompasses a range of elements, including the components of the Internet and networking security and the potential weaknesses associated with them.

This paper extensively explores crucial networking security strategies that play a pivotal role in safeguarding web systems. These strategies include firewalls, credentials, encryption, authentication, and integrity. Additionally, we investigate the architecture of web application assaults, shedding light on various attack methodologies that malicious actors employ. As a result of this research, we examine diverse security protection approaches relevant to high-speed online safety and computer security in the real world. These approaches encompass topics such as DNS security, the use of One-Time Passwords (OTPs) for enhanced authentication, and network defense mechanisms implemented as a collective effort.

Furthermore, this paper conducts an in-depth examination of viral outbreaks in emerging networks and the remarkable pace at which these incidents have been growing.

Motivation: - Cyber-security is a way of protecting devices or websites from malicious sites, links, and attacks that are aimed at stealing information, destroying devices, or money extortion. Implementing effective measures is a challenge since attackers are becoming more efficient. Different attacks like phishing, Ransomware, social engineering, and malware attacks are designed for a specific purpose.

To address these threats, Cybersecurity is typically categorized into three primary domains:

1. **Network Security**: This entails the protection of the network infrastructure, including devices, servers, hosts, and wireless access points. Elements of network security often include firewalls, intrusion detection systems, and other technologies designed to monitor and protect the network.
2. **Cloud Security**: As more data and services are migrated to cloud-based environments, ensuring the security of these cloud systems has become crucial. This includes measures to protect data stored in the cloud and the integrity of cloud-based applications.
3. **Physical Security**: Physical security is an important component, as the physical security of devices and data centers can have a significant impact on overall security. This might include access control, surveillance, and measures to protect hardware and data center facilities.

References: -

https://www.researchgate.net/publication/260793958_Survey_of_Web_Application_and_Internet_Security_Threats