iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41858

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

A Research of Cyber Security and Threats in Emerging Technologies

Ved Prakash Sah Kanu[1], Yusuf Ai Naiem[2], Sudha Shanker Prasad[3]
[1, 2, 3]*Lovely Professional University, Jalandhar G.T Road, Punjab (B.Tech CSE)*

Abstract: ***Cyber security is crucial in the information technology field in today's world. Because every piece of data is now housed online, securing data has become one of the most challenging responsibilities. The first thing that comes to mind when we think of cyber security is cyber criminals, namely hacking, which is on the rise. To tackle cybercrime, several governments and corporations are pursuing several measures. Aside from spectacular attempts, many people still have concerns about cyber security. This study focuses mostly on the issues that cyber security faces with emerging technology. It also concentrates on the most important aspects of data security, such as methods, ethics, and developments that are transforming the public's belief in cyber security.***

Keywords: Cyber security, cybercrime, firewall, social media, cloud computing, and hacking

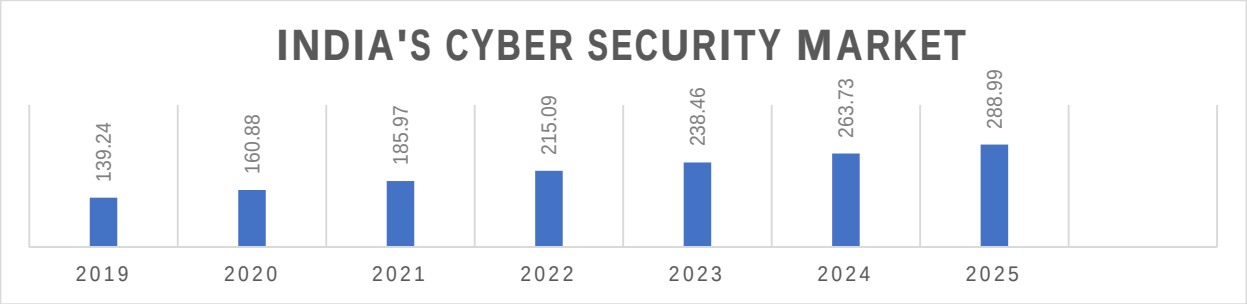
I. INTRODUCTION

Cybersecurity lets us defend internet-connected systems, such as hardware, software, and information, from hacking attempts. Individuals, private enterprises, governments, and organizations use the strategy to secure data centers, businesses, and other networking technologies from unwanted access or attack. Cyber Security Challenges have been increasing rapidly these days, it's the national security in today's world, private and government organizations ranging from small to large enterprises, government universities and private universities, hospitals, all exposed to cyber-attacks from across the world moreover, in dealing with increasingly spreading threats, we frequently encounter enormous hurdles that one must overcome to safeguard their country. Mobile banking, cloud-based services, data science, e-commerce, digital wallets, and other emerging technologies equally need a high degree of safety. Because all these technologies hold extremely sensitive data about people, an individual, or institutions, their confidentiality has become a priority. Strengthening information security and securing crucial information for individuals or institutions are necessary to ensure almost any nation's safety and economic well-being.

II. CYBER SECURITY

Data centers, desktops, smartphones, other electronic devices, and software products simplify all aspects of our lifestyles as our society enters the digital world. Computer systems or connected Smart devices are being used as a core element of critical infrastructures such as healthcare, banking, administration, academics, and industries. Most of these devices can connect to the Internet. Cyber security, also referred to as computer security or information and technology security (IT security), is the protection of information of computers and networks against information leakage or visibility to untrusted sources, along with thievery or malfunction of their hardware, software products, or electronic information, as well as disruption of services or misrepresentation.

Due to the ever-increasing reliance on computer systems, the Online world, and wireless connections like Bluetooth and Wi-Fi, as well as the rapid expansion of smart IoT devices like smartphones and TVs, and thus the numerous gadgets that make up the Internet of things, the field is becoming extremely important. Because of its richness, both in political use and terms of responsibility, Thanks to the advancements in science and innovation, cybersecurity has become one of the most challenging concerns today. Its primary goal is to ensure that the system's reliability, authenticity, and privacy protection are all preserved.



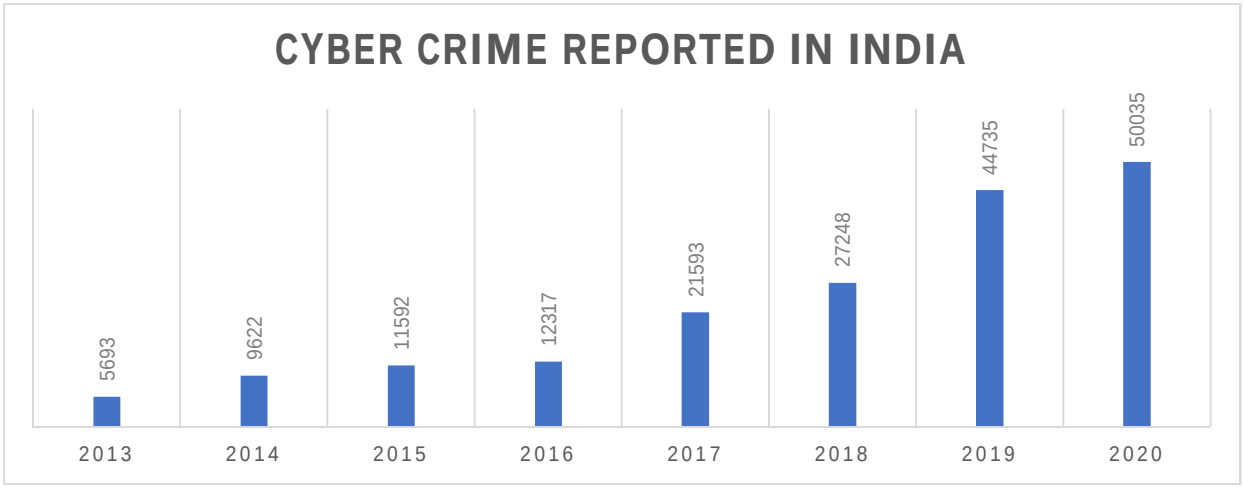
India's cyber security estimated value in 2019, with projections through 2025
Source: Statista

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

III. CYBER CRIME

Cybercrime is a criminal activity that is conducted using computers or the internet. such as committing fraud with innocent people, trafficking in child pornography and intellectual property, stealing personal identities, or violating public privacy. Cybercrime, which is primarily conducted on the Internet, has gained prominence as computers and computer networks have become increasingly important in commerce, entertainment, and governance.

The majority of cybercrime is conducted to obtain information on individuals, businesses, or government officials. Even though these attacks do not target a physical body, they target the personal virtual body, a collection of informational data attributes that describe people and organizations on the internet. In other words, in the digital era, our virtual identities are critical aspects of daily life: our identities are stored in many governments and corporate computer databases. Cybercrime or digital criminals emphasize the importance of networked computers in people's lives, as well as its flaws in the face of established realities like personal identity.



Source: News18

IV. TRENDS CHANGING CYBER SECURITY

With all the Technological Evolution overtaking the world, all companies, local and global, individuals, institutions, and even authorities are leaning on automated systems to run their everyday activities, requiring cybersecurity as a primary obligation to prevent data from malicious internet attacks or unwanted access. As more information about data breaches, ransomware, and cyberattacks becomes accessible to the public, there is a comparable shift in cybersecurity attitudes.

Some of the most important cyber security trends affecting today's society are listed below.

A. Rise of Automotive Hacking

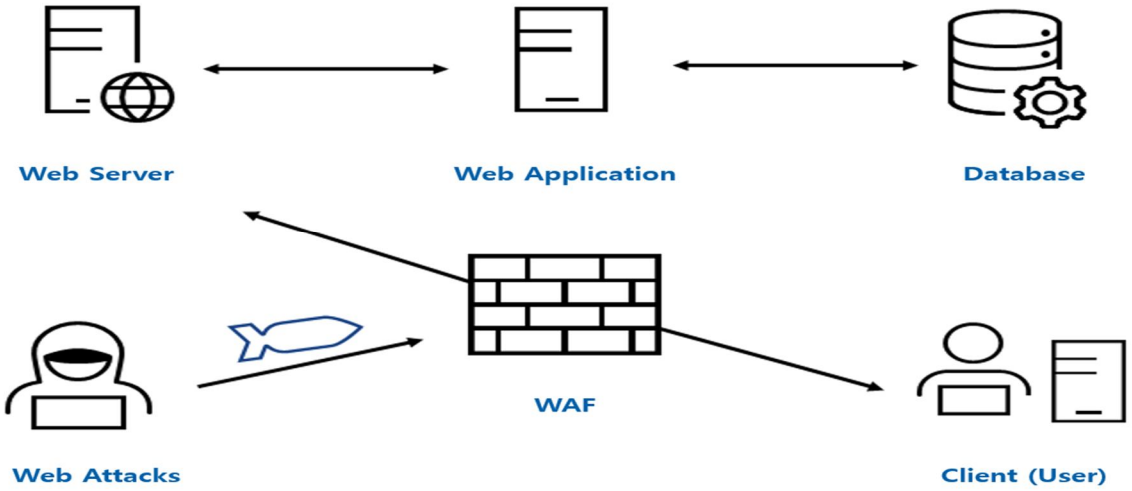
In journey control, machine timing, door cinch, airbags, and advanced systems for motorist backing, modern autos are now crammed with automated software that creates seamless connectivity for motorists. These vehicles use Bluetooth and Wi-Fi technologies to communicate that also opens them to several vulnerabilities or pitfalls from hackers. Gaining control of the vehicle or using microphones for wiretapping is predicted to rise in 2022 with the further use of automated vehicles. Tone-driving or independent vehicles use an indeed further complex medium that requires strict cybersecurity measures. As automotive vehicles use Bluetooth and Wi-Fi technologies to speak, which makes them more susceptible to cyber-attacks. Physical attacks to long-range digital attacks are all possible. Alone in 2020 Last year alone, the amount of automotive hacking incidents jumped by 138%.

B. Cloud Computing and Its Services

Cloud-based services are becoming increasingly popular among small, medium, and big organizations. To look at it another way, cloud computing is becoming increasingly significant all around the world. This new trend poses a severe danger to cyber security because communications may evade established inspection points. As the breadth of software available in the cloud expands, a sound strategy for web apps, as well as cloud organization, will need to adapt to reduce the loss of essential data. Despite cloud service companies' measures to promote their techniques, security issues exist. Despite the cloud's many advantages, it is crucial to remember that as the cloud matures, so do its vulnerabilities.

C. Web Servers

A server is a computer system that manages the hosting of websites. It is a computer program that requisitions and distributes web pages as needed. The primary goal of the webserver is to store, interpret, and distribute online pages to users. This communication is carried through via the Hypertext Transfer Protocol (HTTP). Most of the information on these websites is static content, such as HTML documents, photos, style sheets, and tests. In addition to HTTP, a web server can manage SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol) for email and file transfer and storage.



Source: Pentasecurity.com

Web service attacks that harvest data or send malicious scripts are still a problem. Using hacked respectable websites, cybercriminals spread dangerous software. Data-theft incidents, which are constantly in the headlines, are likewise a critical concern. We must now concentrate on the security of a browser and the web server applications. The best area for these attackers to get data is on web servers. To avoid becoming a victim of these frauds, always use a private browser, especially while making essential transactions.

D. Mobile Networks

We can now connect with anybody, anywhere around the globe. Nevertheless, security has become a significant challenge for such cellular operators. As individuals use more smartphones and tablets, phones, Desktop computers, and other devices, intrusion detection systems, as well as other security measures, become increasingly vulnerable, causing increased security considerations beyond those provided by the programs. Security should always be considered when using these mobile networks. Furthermore, because mobile networks are particularly vulnerable to cybercrime, greater caution is needed in case of a security breach.

E. Encryption of the Code

Data encryption encrypts the data so that it could only be accessed by those who have a secret key (technically known as a decryption key) or passcodes. Information that has not been encrypted is referred to as plaintext, and data that has been encrypted is referred to as ciphertext. Encryption is increasingly becoming one of the most popular and successful data security options for organizations. Asymmetric encryption, often known as public-key encryption, and symmetric encryption are the two basic types of data encryption.

F. Social media's impact on cyber security

As people are becoming more proactive in an increasingly connected world, companies need to develop innovative solutions that protect personal information. Social media has a significant impact on information technology and therefore will take a more active role in personal cyber dangers.

Employees are increasingly using social media, and the potential of a cyberattack is increasing. Because all of them use digital platforms or social networking sites regularly, it has become a significant medium for hackers to steal personal information and sensitive data.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

V. CYBER SECURITY TECHNIQUES

A. Access Control and Password Security

The idea of something like a username and password has traditionally been regarded as a fundamental method of securing personal information. This may be one of the first cyber security measures implemented.

B. Firewalls

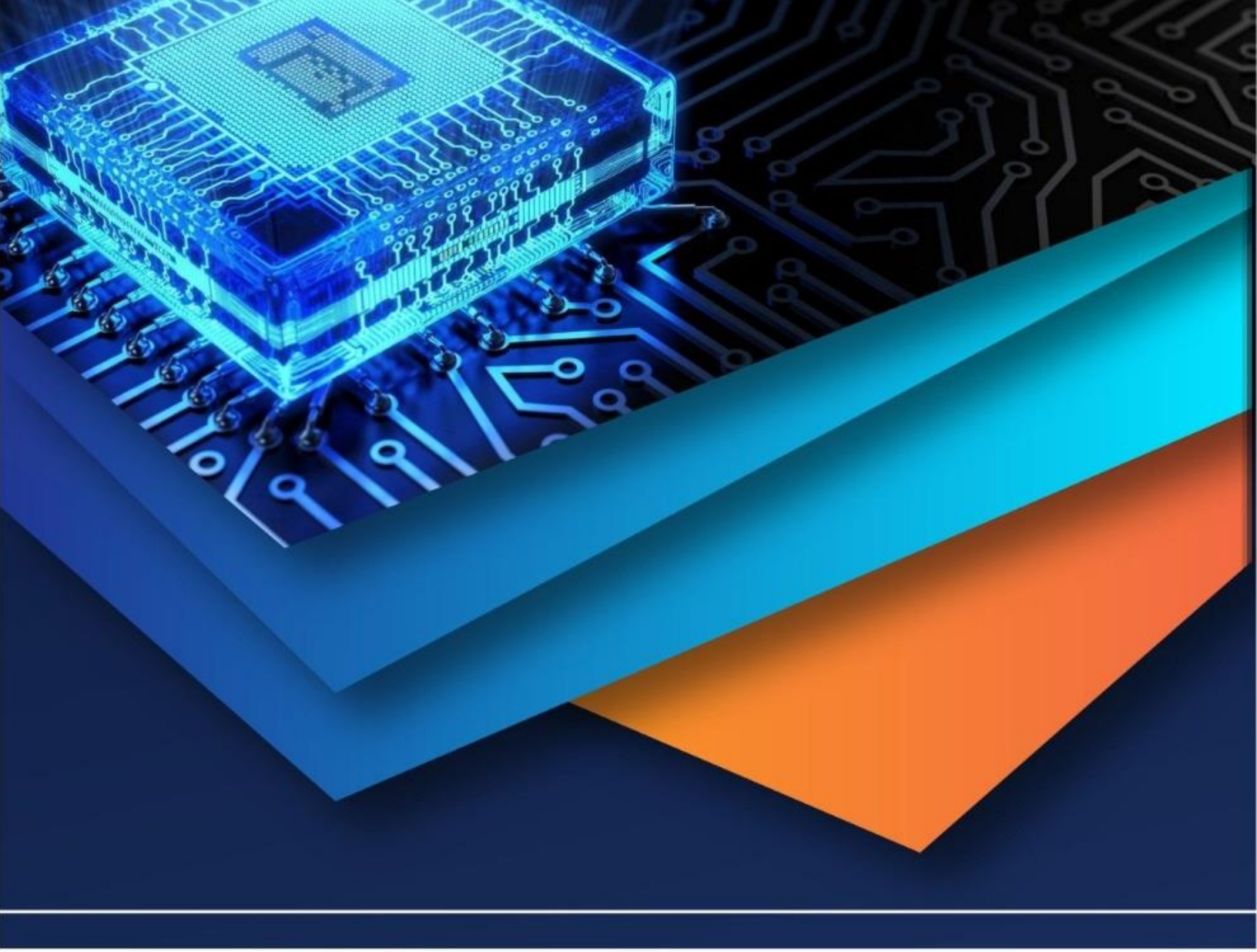
A firewall is a type of code or technology which serves to protect your machine versus Internet-based intruders, malware, and ransomware. All data entering and exiting the Internet must travel via the firewall, which examines each message and rejects those that do not meet security criteria. As more than just a result, firewalls are crucial in the identification of malware.

VI. CONCLUSION

Computer security is a vast topic that is becoming more important as the world gets more interconnected and essential transactions are conducted across networks. With each passing New Year, cybercrime and information security become more distinct. New disruptive technology, as well as cyber tools and threats, appear every year.

REFERENCES

[1] Sunit Belapure Cyber Security: An Introduction Nina Godbole
[2] Audrie Krause's Net Action Report on Non-Profit Organizations' Computer Security Practices
[3] July/August 2013 issue of IEEE Security and Privacy Magazine - IEEECS "Safety Critical Systems — Next Generation."
[4] Avanthi Kumar, CIO Asia, September 3rd, H1 2013: Cyber security in Malaysia



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY