ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

A STUDY ON EMERGING TRENDS ON CYBER SECURITY AND ITS CHALLENGES TO THE SOCIETY AND NEWLY USING TECHNOLOGY

Dr. Deoman Shrikrushna Umbarkar
Associate Professor, Department of Sociology, Late Vasantrao Kolhatkar Arts College, Rohana, Rashtrasant Tukdoji Maharaj Nagpur University,Nagpur

ABSTRACT

Cyber Security plays a very important role within the field of knowledge technology. Our attention is sometimes drawn on "Cyber Security" once we hear regarding "Cyber Crimes". Securing the data became one amongst the most important challenges within the present day. Once ever we expect regarding the cyber security the primary issue that involves our mind is 'cyber crimes' that square measure increasing vastly day by day. Varied Governments and firms square measure taking several measures so as to stop these cyber crimes. Besides varied measures cyber security continues to be an awfully massive concern to several. This paper chiefly focuses on challenges long-faced by cyber security on the most recent technologies. It additionally focuses on latest regarding the cyber security techniques, ethics and also the trends dynamic the face of cyber security. The paper additionally describes the challenges to lack of coordination between Security agencies and also the vital IT Infrastructure.

KEYWORDS: *Cyber Security, Cyber Crime, Cyber Ethics, Social Media, Android Apps.*

INTRODUCTION

In today's Internet-connected world wherever technologies underpin nearly each side of our society, the method of conversion all told aspects of human life, like tending, education, business, etc., has step by step crystal rectifier to the storage of all styles of info, as well as sensitive knowledge. These days web is that the quickest growing infrastructure in way of life. In today's technical surroundings several latest technologies square measure dynamical the face of the person kind. however thanks to these rising technologies we have a tendency to square measure unable to safeguard our personal info in a very effective approach and therefore recently cyber crimes square measure increasing day by day. These days quite sixty percent of total industrial transactions square measure done on-line, therefore this field needed a prime quality of security for clear and best transactions. Therefore cyber security has become a modern issue. The scope of cyber security isn't simply restricted to securing the data in IT trade however conjointly to varied different fields like cyber area etc. Security is that the method of protective the digitized information from felony or from physical harm whereas maintaining the confidentiality and accessibility of knowledge however as technology is growing chop-chop, the law-breaking rate conjointly will increase each in range and quality. The explanation behind this tremendous growth in cyber-crime is that the usage of inadequate computer code, terminated security tools, style flaws, programming errors, simply out there on-line hacking tools, lack of awareness publicly, high rates of monetary returns, etc. so as to explore the vulnerabilities within the target and thereby to attack the victim, additional powerful attack tools square measure developed by the technical attackers. With this, new attacks in several variations square measure returning that square measure tough to observe. Increase in web dependency all told walks of life, digital nature of information in large amounts obtaining accumulated through on-line transactions and decentralization of information repositories, has crystal rectifier to the event of effective security algorithms. The ceaselessly dynamical nature of law-breaking conjointly results in the issue of handling and avoiding rising threats. The task of securing cyber-space is that the most tough and difficult task as advanced threats play a really active role. Therefore, it's necessary to induce insights into the ideas of security defence mechanisms, completely different techniques and trending topics within the space of knowledge security. Even the most recent technologies like mobile computing, E-commerce, internet banking etc conjointly wants high level of security. Since these technologies hold some necessary info relating to someone their security has become a requirement factor. Enhancing cyber security and protective important info infrastructures square measure essential to every nation's security and economic well-being. Creating the net safer (and protective web users) has become integral to the event of latest services still as governmental policy. The fight against cyber crime wants a comprehensive and a safer approach. Provided that technical measures alone cannot forestall any crime, it's important that enforcement agencies square measure allowed to research and prosecute cyber crime effectively. These days several nations and governments square measure imposing strict laws on cyber securities so as to forestall the loss of some necessary information each individual should even be trained on this cyber security and save themselves from these increasing cyber-crimes.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

CYBER CRIME

Cybercrime is criminal activity that either targets or uses a laptop, an electronic network or a networked device. Most, however not all, crime is committed by cybercriminals or hackers UN agency need to create cash. Crime is meted out by people or organizations. Some cyber criminals square measure organized use advanced techniques and square measure extremely technically skilled. Others square measure learner hackers. Rarely, crime aims to break computers for reasons aside from profit. These may well be political or personal. Crime that targets computers typically involves viruses and different styles of malware. Cyber criminals might infect computers with viruses and malware to break devices or stop them operating. They will additionally use malware to delete or steal information. Cyber crime that uses computers to commit different crimes might involve victimization computers or networks to unfold malware, prohibited info or prohibited pictures.

A noted example of a malware attack is that the WannaCry ransomware attack, a worldwide crime committed in might 2017. As day by day technology is enjoying in major role during a person's life the cyber crimes additionally can increase in conjunction with the technological advances.

Cyber Security

Cyber security refers to the body of technologies, processes, and practices designed to shield networks, devices, programs, and knowledge from attack, damage, or unauthorized access. Cyber security might also be brought up as data technology security. Cyber security is very important as a result of government; military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of knowledge on computers and alternative devices. a big portion of that knowledge is sensitive data, whether or not that be property, money knowledge, personal data, or alternative varieties of knowledge that unauthorized access or exposure might have negative consequences. Organizations transmit sensitive knowledge across networks and to alternative devices within the course of doing businesses, and cyber security describe the discipline dedicated to protective that data and also the systems accustomed method or store it because the volume and class of cyber attacks grow, corporations and organizations, particularly those who area unit tasked with safeguarding data regarding national security, health, or money records, ought to take steps to shield their sensitive business and personnel data. As early as March 2013, the nation's high intelligence officers cautioned that cyber attacks and digital spying area unit the highest threat to national security, eclipsing even terrorist act challenges of cyber security for an efficient cyber security, a company has to coordinate its efforts throughout its entire system.

Elements of cyber encompass all of the following:

Network security: The process of protecting the network from unwanted users, attacks and intrusions.

- **Application security:** Apps require constant updates and testing to ensure these programs are secure from attacks.
- **Endpoint security:** Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.
- **Data security:** Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- **Identity management:** Essentially, this is a process of understanding the access every individual has in an organization.
- **Database and infrastructure security:** Everything in a network involves databases and physical equipment. Protecting these devices is equally important.
- **Cloud security:** Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large amount of challenges.
- **Mobile security:** Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- **Disaster recovery/business continuity planning:** In the event of a breach, natural disaster or other event data must be protected and business must go on. For this, you'll need a plan. End-user education: Users may be employees accessing the network or customers logging on to a company app educating good habits (password changes, 2-factor authentication, etc.) is an important part of cyber security.

The toughest challenge in cyber security is that the ever-evolving nature of security risks themselves historically, organizations and therefore the government have centered most of their cyber security resources on perimeter security to guard solely their most important system elements and defend against celebrated treats. Today, this approach is lean, because the threats advance and alter additional quickly than organizations will maintain with. As a result, consolatory organizations promote additional proactive and adaptation approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued tips in its risk assessment framework that advocate a shift toward continuous observation and period assessments, a data-focused approach to security as opposition the standard perimeter-based model.

CYBER SECURITY TECHNIQUES

Access control and password security

If threat actors can't access your network, the quantities of harm they'll be ready to do are extraordinarily restricted. Additionally to preventing unauthorized access, bear in mind that even licensed users may also be potential threats. Access management permits you to extend your network security by limiting user access and resources to solely the components of the network that directly apply to individual users' responsibilities. The users limit their access or to line the sturdy countersign for security purpose.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Authentication of data

This elementary cyber security technique intends to verify the identity of user supported the credentials hold on within the security domain of the system. the foremost common mode of governance is positive identification technology, the most challenge encountered in authenticating method is thwarting tries of unauthorized individuals to pay attention to the authenticating message. The positive identification transmitted over AN insecure medium is vulnerable to be intercepted by dishonest those that will use it to disguise because the original user. This downside is countered by coding.

Malware scanners

Malware Scanning is that the method of detecting malware within the laptop to eliminate it. It's as a result of malware scanning that the threats lurking on the pc are known. While not malware scanning, the pc is in danger of malware infection.

It sporadically scans the pc to find and defeat any malware that may have slipped through. It's frequently updated to acknowledge the most recent threats. A laptop that's not scanned frequently might have already got malware infection solely it doesn't show any sign of malware nevertheless.

Firewalls

If threat actors can't access your network, the quantities of harm they'll be ready to do are extraordinarily restricted. However additionally to preventing unauthorized access, bear in mind that even licensed users may also be potential threats. Access management permits you to extend your network security by limiting user access and resources to solely the components of the network that directly apply to individual users responsibilities.

Anti-Virus Software

The threats of laptop or desktop computer viruses or undesirable short programs that trigger unwanted commands while not the specific consent of user have assumed monstrous proportions. Anti-virus package carries out 2 functions; it prevents the installation of virus during a system and scans the systems for viruses that are already put in. Most viruses are created to focus on Windows OS because it is that the most popular computing platform of plenty. Apple and operational system users can even return beneath the attack of viruses completely engineered for such operating systems.

Digital Signatures

Digital signatures is erected out of constant mathematical algorithms that are utilized in uneven encoding. A user is unengaged to take a look at that he possesses a non-public key by obtaining some info encoded with it. Anyone will get constant decrypted by having the general public key which will verify the person's credentials. This method is in essence the precise reciprocal of public key encoding and likewise functions on the idea that the approved user solely has the non-public key.

TRENDS CHANGING CYBER SECURITY

In this paper mentioned there are some of the trends that are having a vast impact on cyber security.

Web Servers

The threat of attacks on net applications to extract information or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate net servers they've compromised however data-stealing attacks, many of that get the eye of media, are an enormous threat. Now, we'd like a bigger stress on protective net servers and net applications. Net servers are particularly the most effective platform for these cyber criminals to steal the info. Thus one should use a safer browser particularly throughout necessary transactions so as to not fall as a prey for these crimes.

Mobile Networks

Today we have a tendency to are ready to hook up with anyone in any a part of the globe. Except for these mobile networks security may be a terribly massive concern. Recently firewalls and alternative security measures have become porous as folks are exploitation devices like tablets, phones, PC's etc all of that once more need further securities except those gifts within the applications used we have a tendency to should always have confidence the protection problems with these mobile networks more mobile networks are extremely susceptible to these cyber crimes plenty of care should be taken just in case of their security problems.

New Internet Protocol: IPv6

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 10| October 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

media is among the emerging risks identified in *Global Risks 2013* report. Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

Challenges

Digitalization or The use of e-resources more and more impacts all aspects of our lives and industries. We notice to area unit seeing the speedy adoption of machine learning and AI tools, similarly as Associate in Nursing increasing dependency on software package, hardware and cloud infrastructure.

Conclusion

Computer security may be a huge topic that's changing into a lot of necessary as a result of the globe is changing into extremely interconnected, with networks being employed to hold out vital transactions. Cyber crime continues to diverge down totally different ways with every New Year that passes so will the protection of the data. the most recent and troubled technologies, in conjunction with the new cyber tools and threats that come back to lightweight daily, area unit difficult organizations with not solely however they secure their infrastructure, however they need new platforms and intelligence to try to thus there is no good resolution for cyber crimes however we should always strive our boundary to reduce them so as to possess a secure and secure future in cyber area.

REFERENCES

1. *Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1-ISSN 2229-5518.*
2. *Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011*
3. *Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole*
4. *A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.*
5. *Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole*
6. *A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.*
7. *International Journal of Scientific & Engineering Research, Volume 4, Issue September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy*
8. *IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.*
9. *http://www.crossdomainsolutions.com/cyber-security/tools-techniques/*