IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, October 2024

Cybersecurity: A Review of Tactics, Trends, and Prevention Strategies

Krishna
Research Scholar, Darbhanga, India
krishna.dbg99@gmail.com

Abstract: *The digital revolution has fostered an interconnected world, with internet users exceeding 4.66 billion in 2021. This hyper-connectivity has revolutionized communication and information exchange, but it has also created a fertile ground for cybercrime. As the volume of sensitive data traversing the internet explodes, robust cybersecurity measures are no longer a luxury, but a necessity. This paper argues that "Cybersecurity Awareness" is a cornerstone in fortifying our digital infrastructure. However, achieving effective cybersecurity requires a multifaceted approach. This paper delves into the critical relationship between cyber security recognition, the development of essential skills, and the consistent application of those skills in proactive defence. Research suggests a concerning disconnect: while individuals may possess basic cyber awareness, they often fail to translate this knowledge into concrete actions, particularly those perceived as inconvenient. This highlights the need to bridge the gap between theoretical understanding and practical implementation. The paper establishes a direct correlation between cyber awareness and cyber knowledge, emphasizing that cultivating deeper knowledge fosters greater awareness and empowers users to make informed security decisions.*

To equip users with the necessary tools, the paper explores various cyberattack methodologies employed by malicious actors. By understanding these methods, users can identify vulnerabilities within their own digital ecosystems. Additionally, the paper examines vulnerability detection techniques, empowering individuals to proactively mitigate potential threats. Finally, the paper outlines promising avenues for future research in cybersecurity awareness programs, paving the way for the development of more engaging, targeted, and effective educational initiatives.

Keywords: Cyber Security, Threats, Security Models and Feasible solutions

I. INTRODUCTION

The digital age has ushered in an era of unprecedented connectivity, marked by a proliferation of online platforms. Social media, defined as "a group of Internet-based applications that allow the creation and exchange of User Generated Content" [2], has become an integral part of daily life, fostering communication and engagement on a global scale. Platforms like Facebook, Twitter, WhatsApp, and LinkedIn have revolutionized the way we connect, offering unparalleled convenience and ease of communication

However, this interconnectedness comes at a cost. The very nature of social media, which thrives on user-generated content and information sharing, creates vulnerabilities that cybercriminals can exploit. Users often share sensitive information on these platforms, including location data, financial details, and personal identifiers, making them prime targets for malicious attacks. Cybersecurity, at its core, isabout safeguarding "the security and privacy of digital assets" – everything from networks and devices to the information exchanged online [5]. While advancements in technology have led to the development of data protection protocols, such as the "Possible Location Deployment Protocol (PLDP)" for Wireless Sensor Networks (WSNs) that enhances network resilience [6], absolute security remains an elusive goal [4].

The onus of cybersecurity extends beyond technological solutions. Cultivating a culture of cybersecurity awareness among social media users is equally crucial. Organizations are increasingly recognizing this need and are investing in educational initiatives to empower individuals to navigate the digital landscape safely.The massive volume of data shared on social media platforms necessitates a collaborative approach. While ongoing research strives to develop

DOI: 10.48175/IJARSCT-19728

robust security solutions like large-scale underwater sensor network architectures [7], the focus must also shift towards user education. By equipping users with the knowledge and tools to identify and mitigate online threats, we can collectively build a more secure and resilient digital ecosystem.

II. NETWORK SAFETY: CURRENT PERSPECTIVES

The digital revolution has fundamentally reshaped our world, fostered unprecedented global connectivity, and transformed communication, commerce, and information access. However, this interconnectedness comes at a cost. The vast expanse of the internet, while brimming with opportunity, also presents a complex and ever-evolving threat landscape that necessitates a multi-pronged approach to network safety.

At its core, network safety refers to the "protection against undesirable disclosure, destruction, or modification of data in a system and also the protection of systems themselves" [8]. Unfortunately, malicious actors – from state-sponsored groups to independent hackers – constantly exploit vulnerabilities to compromise online systems and steal sensitive data.

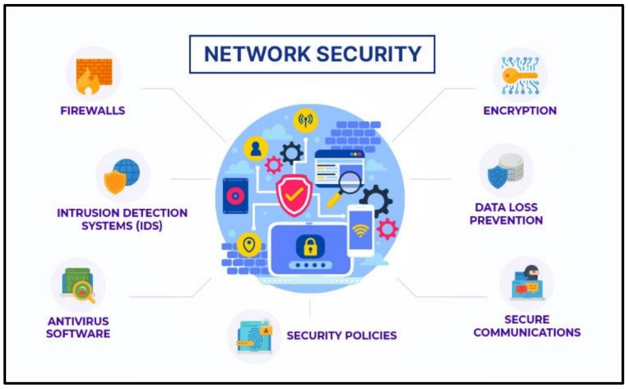

Fig 1. Multiple system of data security approaches [14].

The spread of misinformation and disinformation campaigns poses a significant threat to network safety. As highlighted by the World Economic Forum in their 2013 report [10], these campaigns can manipulate public opinion, sow discord, and erode trust in democratic institutions. Social media platforms, with their vast reach and echo chamber effects, can unwittingly serve as breeding grounds for such campaigns.

Phishing scams remain a persistent threat, preying on human vulnerabilities and leveraging social engineering tactics to trick users into revealing sensitive information or clicking on malicious links. These emails or messages can appear deceptively legitimate, often mimicking trusted sources like banks or social media platforms, making them particularly dangerous for unsuspecting users [12].

Denial-of-Service (DoS) attacks aim to disrupt user access to a system or service by overwhelming it with traffic. These attacks, along with more sophisticated Distributed DoS (DDoS) attacks, can cripple critical infrastructure like online banking systems or e-commerce platforms. Data breaches, where unauthorized access is gained to sensitive user information, pose another significant threat. Breached data can be used for identity theft, financial fraud, or further cyberattacks. These attacks compromise the confidentiality, integrity, and availability (CIA triad) of online data, jeopardizing trust in online platforms and services [13].

While technological advancements play a vital role in network safety, a comprehensive approach is necessary. Cryptographic algorithms, can scramble data to render it unreadable without a decryption key, offering a crucial layer of protection [14]. However, robust security solutions extend beyond technology. Cultivating a culture of cybersecurity awareness among users is equally important. Educating individuals on identifying phishing attempts, employing strong passwords and multi-factor authentication, keeping software updated, and practicing safe online habits empowers them to become active participants in their own online security.

Network safety is a shared responsibility. Governments, industry leaders, and cybersecurity professionals must collaborate to create a more secure digital ecosystem. Governments can establish regulatory frameworks to hold malicious actors accountable and promote responsible cybersecurity practices. Industry leaders have a responsibility to

ISSN 2581-9429 IJARSCT

DOI: 10.48175/IJARSCT-19728

invest in robust security measures and develop user-friendly security tools. Cybersecurity professionals play a vital role in developing cutting-edge threat detection and mitigation strategies, staying ahead of cyber adversaries.

Network safety remains a dynamic field, demanding continuous innovation. Research and development in areas like intrusion detection systems, threat intelligence, and security protocols are essential to stay ahead of cyber threats. Emerging technologies like artificial intelligence and machine learning hold promise for automating threat detection and response, but require careful consideration of potential biases and ethical implications.

By fostering a collaborative defence that combines technological advancements with user education and public-private partnerships, we can build a more resilient digital infrastructure. Network safety is an ongoing journey, not a destination. By remaining vigilant, adapting to evolving threats, and working together, we can create a safer and more secure online environment for everyone.

III. SECURITY MODELS

Security models provide a foundational framework for safeguarding information systems. They define the guiding principles and mechanisms to ensure the confidentiality, integrity, and availability (CIA triad) of data. Understanding these models is crucial for building robust security architectures.

A. Security by Layers:

Security is not a single point of defense but a layered approach. Visualize a security system as a fortified castle, with each layer adding another line of defense.

Let's explore these layers from the inside out:

Table I. Summary of Security layers

Security Layers	Uses of Layers
Cryptographic Algorithms	This layer forms the bedrock of secure communication. Algorithms like RSA, AES, and DES perform encryption and decryption, scrambling data into an unreadable format for unauthorized users. Public-key and private-key cryptography work in tandem to ensure secure key exchange and digital signatures.
Network Security Protocols	Building upon the encryption foundation, Layer 3 implements cryptographic primitives like hashing and digital signatures. These protocols, like Secure Sockets Layer (SSL)/Transport Layer Security (TLS), establish secure connections and verify data integrity during transmission.
Transport Layer Security:	This layer focuses on core security services. Protocols like OpenVPN create secure tunnels for encrypted data transmission, ensuring confidentiality and data integrity.
Application Security	The outermost layer interacts directly with users and applications. Secure applications like firewalls and email encryption services act as gatekeepers, filtering incoming and outgoing traffic based on pre-defined security rules. Common security vulnerabilities like SQL injection and DDoS attacks often target this layer.

While the layered model provides a valuable framework, security extends beyond technology. User education is paramount. Teaching users to identify phishing attempts, maintain strong passwords, and practice safe browsing habits empowers them to actively contribute to their own online security.

Building a secure digital ecosystem necessitates collaboration. Governments can establish regulations, industry leaders can invest in security measures, and cybersecurity professionals can develop innovative solutions to stay ahead of evolving threats.

Security models offer a roadmap for navigating the complex landscape of cybersecurity. By understanding the layered approach and fostering a culture of security awareness, we can work together to create a more secure and resilient digital world.

DOI: 10.48175/IJARSCT-19728

IV. DIGITAL RISKS OVER ONLINE PLATFORMS

The vast expanse of the web offers a wealth of information and connectivity, but it also harbours a multitude of cybersecurity threats. Understanding these threats and implementing robust security measures are crucial for safeguarding our devices, data, and privacy in the digital age [9].

Cyber threats can be broadly categorized into two main types, each with its own objectives and tactics:

Operation-Oriented Attacks:

These attacks target the infrastructure of online systems and services, aiming to disrupt operations, steal critical data, or damage their reputation. Malicious actors may employ various techniques:

Table II. Techquies of operation-oriented attacks

Techquies of operation-oriented attacks	Description
Defacement	Vandalizing websites by altering content or displaying malicious messages, potentially causing confusion and distrust among users.
Distributed Denial-of-Service (DDoS) Attacks	Overwhelming websites or online services with a flood of traffic, rendering them inaccessible to legitimate users and hindering core functionalities. These attacks can cripple critical online infrastructure during peak usage times, such as online banking platforms during holidays or e-commerce sites on sale days, causing significant inconvenience and reputational damage.
Unauthorized Access	Exploiting vulnerabilities in software or system security measures to infiltrate computer systems and steal user data, including personal information, login credentials, or financial details. This stolen data can be used for identity theft, financial fraud, or further cyberattacks.

User-Targeted Attacks:

These attacks exploit human vulnerabilities to compromise individual devices or steal personal information. Common tactics include:

Table III. Techquies of User-targeted attacks

Techquies of User-targeted attacks	Description
Social Engineering	Social engineering is a particularly potent weapon in the cybercriminal arsenal. By exploiting trust and leveraging user psychology, attackers can gain access to sensitive information or spread malware disguised as legitimate content.
Malware and Phishing	Deception tactics that lure users into downloading malicious software (malware) or clicking on phishing links. Malware can infect devices, steal data, disrupt normal operations, or hold data hostage through ransomware attacks. Phishing links often lead to fraudulent websites designed to trick users into entering login credentials or other sensitive information that can then be used for unauthorized access.
Spam and Disinformation Campaigns	Flooding users with unwanted emails (spam) or spreading false information (disinformation) to disrupt communication, manipulate public opinion, or sow discord. Spam messages can be intrusive and annoying, but can also be used to deliver malware or phishing links.

Mobile Devices: A Growing Target with Unique Vulnerabilities

The increasing popularity of mobile devices for web browsing and online activities creates unique security concerns. Mobile devices are often less secure than traditional computers due to factors like:

Table IV. Mobile Devices: A threat

Mobile Devices	Description
Smaller screen sizes	Making it easier to miss red flags in emails or messages such as typos in URLs or grammatical errors in phishing attempts.
Limited processing power	Hinders real-time threat detection by security software leaving devices vulnerable during the time it takes for security software to identify and neutralize a threat.
Prevalence of third-party app stores	These stores may not have the same level of security vetting as official app stores increasing the risk of downloading malware-laden apps. Malicious apps can steal user data. install additional malware or disrupt device functionality

These factors make mobile devices vulnerable to malware attacks embedded in third-party apps. Furthermore, websites themselves can be compromised, exposing user data or installing malware on devices that visit the site. Malicious actors may exploit vulnerabilities in mobile operating systems or web browsers to infect devices.

Other types of attacks:

Cyberattacks are not isolated incidents; they can trigger a cascade of negative consequences that extend far beyond the initial target. Stolen user data, a frequent byproduct of cyberattacks, acts as the fuel that ignites this ripple effect, causing widespread damage [4]. Let us delve deeper into the far-reaching effects of stolen user data:

Table V. *O*ther types of attacks

Attacks	Description
Identity Theft	Stolen user data, which can include names, addresses, Social Security numbers, credit card details, and even medical records, becomes a goldmine for cybercriminals. Attackers can assume the victim's identity to open new accounts, obtain credit cards, or even secure loans, leaving the victim with a mountain of debt and a damaged credit score.
Financial fraud	Stolen financial information can be used to make unauthorized purchases, drain bank accounts, or even initiate illegal money transfers.
Reputational Damage	Data breaches can severely tarnish the reputation of organizations that fall victim to cyberattacks. Customers may lose trust in a company's ability to safeguard their personal information, leading to a decline in business and brand loyalty.
Blackmail and Extortion	Stolen data, especially personal or sensitive information, can be used for blackmail and extortion purposes. Attackers may threaten to expose embarrassing information, leak medical records, or damage a victim's reputation unless a ransom is paid. This can have a devastating impact on individuals, families, and even corporations.
Psychological Impact	Victims of cyberattacks, especially those who have had their personal information stolen, can experience a range of psychological effects, including anxiety, depression, and even post-traumatic stress disorder (PTSD). The fear of identity theft, financial losses, and the violation of privacy can take a significant toll on mental well-being.
Disruption of Critical Services	Cyberattacks can cripple critical infrastructure and disrupt essential services. For example, an attack on a power grid could leave entire cities without electricity, while an attack on a healthcare system could disrupt patient care and put lives at risk. The ripple effects of these attacks can be widespread and devastating.

V. FEASIBLE SOLUTIONS FOR CYBER SECURITY

The digital age offers a wealth of opportunities for connection, communication, and innovation. However, this interconnectedness also creates a complex and ever-evolving landscape of cybersecurity threats. Data breaches, malware attacks, phishing scams, and ransomware assaults are just a few examples of the challenges organizations and individuals face.

In today's digital age, data has become a valuable commodity, and user data is the new battleground for cybercriminals. The ease with which data can be stolen and sold on the dark web fuels this illicit industry. Furthermore, the interconnectedness of our digital world means that a single cyberattack can have cascading effects across various sectors and regions.

Recognizing the far-reaching consequences of cyberattacks is crucial. Organizations and individuals alike can take steps to mitigate the ripple effect by:

- Implementing robust cybersecurity measures to protect data
- Educating users about cyber threats and best practices for online safety
- Having a data breach response plan in place to minimize damage in case of an attack
- Advocating for stronger data privacy regulations

By working together, we can build a more secure digital ecosystem and reduce the collateral damage caused by cyberattacks.

Fortunately, there are a multitude of practical solutions and advanced technologies available to mitigate these risks and build a more secure digital environment. Here is a comprehensive look at how both individuals and organizations can bolster their cybersecurity posture:

A. For Individual Users: Building a Wall of Défense:

Precaution Steps	Description
Cultivate Cybersecurity Awareness:	Knowledge is power. Educate yourself about common cyber threats and social engineering tactics. Stay informed about the latest security vulnerabilities and software updates. This empowers you to identify red flags and take proactive measures to protect yourself from falling victim to online scams and attacks.
Practice Secure Online Habits:	Develop and maintain safe online habits. Scrutinize emails and attachments carefully, especially those from unknown senders. Don't click on suspicious links or download unsolicited attachments. Be cautious about what information you share online, especially on public forums or social media platforms. Even with privacy settings enabled, exercise discretion when sharing personal details.
Embrace Strong Passwords and Multi-Factor Authentication (MFA):	Move away from weak, easily guessable passwords. Instead, utilize strong, unique passwords for all your online accounts and change them regularly. Consider using a password manager to generate and store complex passwords securely. Whenever possible, enable two-factor authentication (2FA) on your online accounts.
Secure Your Devices and Home Network:	Mobile devices are often more vulnerable than traditional computers. Download apps only from trusted sources like official app stores. Exercise caution when clicking on links or opening attachments, especially on emails or messages. For your home network, use a strong password for your Wi-Fi network and enable network encryption (WPA2 or WPA3) to shield your devices from unauthorized access.

Table V. Steps for Induvial users

B. For Organizations: Building a Wall of Défense:

Fortifying the Digital Perimeter Invest in Security Awareness Training: Empower your employees to become the first line of defence. Regularly educate them about cybersecurity best practices. Train them to identify and avoid phishing

DOI: 10.48175/IJARSCT-19728

attempts, social engineering tactics, and malware threats. By fostering a culture of security awareness within your organization, you significantly reduce the risk of human error that can be exploited by attackers.

Table VI. Steps for Organization

Precaution Steps	**Description**
Enforce Robust Password Policies:	Weak passwords are a gateway for cyberattacks. Enforce strong password policies within your organization, requiring employees to use complex, unique passwords and change them regularly. Consider implementing a password management solution for increased security and to streamline password management for employees.
Maintain Software Updates:	Cybercriminals are constantly looking for vulnerabilities in outdated software. Ensure all devices and software used by the organization are kept up-to-date with the latest security patches. This critical step helps to mitigate vulnerabilities that could be exploited by attackers to gain unauthorized access to your systems and data.
Implement Data Loss Prevention (DLP):	Protecting sensitive data is paramount. Consider implementing Data Loss Prevention (DLP) solutions to monitor and control the flow of sensitive data within your organization. DLP can help prevent accidental or intentional data leaks through email, social media, or other channels.
Leveraging the Power of Advanced Technologies:	Incorporate advanced technologies like network analysis, anomaly detection, machine learning, and artificial intelligence (AI) to bolster your defenses.

C. Miscellaneous Methods:

Table VII. Miscellaneous Method for analysis

Methods	**Description**
Network analysis:	Continuously monitor network traffic for suspicious activity, such as unauthorized access attempts, data exfiltration attempts, or unusual traffic patterns. Network analysis tools can help identify potential threats in Realtime, allowing for a swift response.
Anomaly detection:	Utilize AI-powered anomaly detection systems to identify deviations from normal user behaviour, network activity, or system configurations. These deviations could potentially signal a cyberattack in progress.
Implement a Layered Security Approach:	A single security measure is rarely enough. Implement a layered security approach that combines firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint protection software, and data encryption to create a comprehensive defense against cyberattacks.

Cybersecurity is not a one-time fix; it's an ongoing process that requires continuous vigilance and adaptation. Organizations and individuals must stay informed about evolving threats and adapt

VI. THE CRUCIAL ROLE OF AI AND MACHINE LEARNING IN CYBERSECURITY

The ever-evolving threat landscape of cybersecurity demands innovative solutions. Artificial intelligence (AI) and machine learning (ML) are emerging as powerful tools in the fight against cyberattacks. Here's a breakdown of how these technologies are revolutionizing cybersecurity:

Harnessing the Power of Big Data:

*T*raditional security methods struggle to keep pace with the massive volume and complexity of cyber threats. AI and ML excel at processing vast amounts of data, including network traffic logs, system events, and malware samples.

These technologies can identify patterns and anomalies that might go unnoticed by human analysts, enabling proactive threat detection.

Machine Learning for Advanced Threat Detection:

- Anomaly Detection: ML algorithms can learn the typical behaviour of users, devices, and network traffic. Deviations from this baseline behaviour could indicate a potential attack, allowing for a faster response.
- Vulnerability Detection: ML can analyse vast code repositories to identify potential vulnerabilities in software before they can be exploited by attackers.
- Botnet Detection: Sophisticated botnet detection methods leverage machine learning to identify coordinated activity among compromised devices, helping to dismantle botnets used in large-scale attacks.
- Real-Time Threat Analysis and Response:The speed and efficiency of AI and ML are crucial advantages in cybersecurity. These technologies can analyze data in real-time, enabling automated security systems to detect and respond to threats much faster than traditional methods. This rapid response can significantly minimize the damage caused by a cyberattack.
- AI-powered Threat Hunting:AI can assist security analysts in the proactive hunt for threats. By analyzing vast amounts of data, AI can identify potential threats that might be missed by human analysts due to fatigue or the sheer volume of information. This allows security teams to focus their efforts on high-priority threats.
- Beyond Detection: Predictive Capabilities: Machine learning algorithms can analyze historical data and threat intelligence to predict future attacks. This enables organizations to take preventive measures and harden their defences against anticipated threats.

Examples of AI and ML Applications in Cybersecurity

Some types of examples of ai and ml applicationsin cybersecurity*:*

Table VIII. Applications in cybersecurity

Applications in cybersecurity	**Description**
Email Security:	AI can analyze email content and sender behaviour to identify and filter out phishing attempts.
Endpoint Security:	Machine learning algorithms can monitor endpoint devices for suspicious activity, such as malware execution or unauthorized data access attempts.
Intrusion Detection/Prevention Systems (IDS/IPS):	AI-powered IDS/IPS systems can analyze network traffic in real-time to detect and prevent intrusions [18].

D. Challenges and Considerations:

While AI and ML offer immense potential for cybersecurity [9], there are challenges to consider:

Table IX. Challenges in cybersecurity

Challenges	**Description**
Data Quality and Bias:	The effectiveness of AI and ML heavily relies on the quality and quantity of data used to train the models. Biased data can lead to biased models, potentially overlooking certain types of attacks.
Explainability and Transparency:	Understanding how AI models arrive at their decisions is crucial for building trust and ensuring they are not making critical errors.
The Evolving Threat Landscape:	Attackers are constantly adapting their tactics. Cybersecurity solutions powered by AI and ML must be continuously updated and improved to stay ahead of evolving threats.

DOI: 10.48175/IJARSCT-19728

VII. CONCLUSION AND FUTURE SCOPE

The digital age presents a double-edged sword. It offers unparalleled connectivity and innovation but also exposes us to a complex and ever-evolving landscape of cyber threats. As we rely more heavily on online platforms, robust cybersecurity becomes paramount.Securing the digital future requires a multi-pronged approach. Individuals must practice safe online habits, cultivate cybersecurity awareness, and utilize strong passwords and multi-factor authentication. Organizations need to invest in security awareness training for employees, enforce robust password policies, and implement comprehensive security solutions that leverage advanced technologies like network analysis, anomaly detection, machine learning, and artificial intelligence.Collaboration between individuals, organizations, and governments is crucial to develop effective strategies to combat cybercrime [19].

The cybersecurity landscape is constantly evolving. As attackers develop new techniques, so too must our defenses. The future of cybersecurity lies in continuous innovation and adaptation. Here are some promising areas for future development:

Future Development Scopes	**Description**
Automated Incident Response: AI	powered systems will be able to not only detect threats but also take automated actions to contain and mitigate them, minimizing human error and response times.
Self-Learning Security Systems:	Security systems will continuously learn and adapt to new threats and attack methodologies, providing a more dynamic defense posture.
Human-AI Collaboration:	Security analysts will leverage AI tools to improve their efficiency and effectiveness in threat hunting and incident response, fostering a powerful partnership between human expertise and machine intelligence.

Technology plays a vital role, but it's only part of the solution. Building a culture of security awareness across individuals and organizations is essential. By fostering a shared understanding of cyber threats and best practices, we can create a more secure digital environment for everyone.

The digital age offers immense opportunities, but it also comes with inherent risks. By adopting a multi-layered approach that combines technological advancements, user education, and collaborative efforts, we can build a more secure and resilient digital future.

In conclusion, AI and machine learning are revolutionizing the fight against cyberattacks. By leveraging these powerful technologies, organizations can significantly enhance their security posture and protect themselves from an ever-increasing array of threats. However, it's crucial to address the challenges associated with AI and ML to ensure their responsible and effective implementation in the field of cybersecurity.

REFERENCES

[1]. Gutzwiller, R.S., Fugate, S., Sawyer, B.D. and Hancock, P.A., 2015, September. The human factors of cyber network defense. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 59, No. 1, pp. 322-326). Sage CA: Los Angeles, CA: SAGE publications.

[2]. Prayitno, O.T., da Costa Tavares, O.C., Damaini, A.A. and Setyohadi, D.B., 2017, October. Regulatory framework creation analysis to reduce security risks the use of social media in companies. In 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE) (pp. 235-238). IEEE.

[3]. de Paula, A.M., 2009, January. Security aspects and future trends of social networks. In Proceedings of the fourth international conference of forensic computer science (pp. 66-77).

[4]. Rani, E.P., A Review Paper on Cyber Crime 2018.

[5]. McKenzie, T.M., 2017. Is cyber deterrence possible? Air University Press.

[6]. Bindal, A.K., Mangla, A., Prasad, D. and Patel, R.B., 2012, December. PLDP: Possible Location Deployment Protocol for Energy Harvesting in WSNs. In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (pp. 574-579). IEEE. [7]Bindal, A., 2020. 3-tier architecture for sustainable underwater wireless sensor networks. Adv. Math.: Sci. J, 9(3), pp.1205-1212. [8]Gurusamy, V. and Hirani, B., 2018. Cyber security for our digital life. In Proceeding: National Conference on Innovations in Computer Technology and its Applications, Guru Nanak College, Chennai.

[7]. Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H. and Elkhediri, S., 2019, May. Cybersecurity: A review of internet of things (IoT) security issues, challenges, and techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

[8]. Thakur, K., Hayajneh, T. and Tseng, J., 2019. Cyber security in social media: challenges and the way forward. IT Professional, 21(2), pp.41-49.

[9]. Hayes, N., 2017. Why social media sites are the new cyber weapons of choice.

[10]. Reid, R. and Van Niekerk, J., 2016. Decoding audience interpretations of awareness campaign messages. Information & Computer Security.

[11]. Safa, N.S., Maple, C., Watson, T. and Von Solms, R., 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of information security and applications, 40, pp.247-257.

[12]. Gohel, H.A., Kadivar, M. and Virpariya, P.V., Penetration Study Of Threats And Attacks Of Online Social Security 2011.

[13]. Teplinsky, M.J., 2012. Fiddling on the roof: Recent developments in cybersecurity. Am. U. Bus. L. Rev., 2, p.225.

[14]. Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H., Marufuzzaman, M. and Bian, L., 2017. Botnet detection using graph-based feature clustering. Journal of Big Data, 4(1), pp.1-23.

[15]. Neethu, B., 2013. Adaptive intrusion detection using machine learning. International Journal of Computer Science and Network Security (IJCSNS), 13(3), p.118.

[16]. Lenkart, J.J., 2011. The vulnerability of social networking media and the insider threat: New eyes for bad guys. Naval Postgraduate School Monterey Ca Dept Of National Security Affairs.

[17]. Nerney, C., 5. Top social media security threats," 2011. [21]Teplinsky, M.J., 2012. Fiddling on the roof: Recent developments in cybersecurity. Am. U. Bus. L. Rev., 2, p.225.

DOI: 10.48175/IJARSCT-19728