Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Emerging Cyber Threats: Comprehensive Analysis and Solutions

[1] Chirag Maheshwari, [2] Shafiqul Abidin, [3] Mohd Saud

[1]Department of Computer Science, Aligarh Muslim University,

Aligarh-202002, Uttar Pradesh, India

chirag.maheshwari135408@gmail.com

[2]Department of Computer Science, Aligarh Muslim University,

Aligarh-202002, Uttar Pradesh, India

shafiqulabidin@yahoo.co.in

[3]Department of Computer Science, Aligarh Muslim University,

Aligarh-202002, Uttar Pradesh, India

saudmohd862@gmail.com

ARTICLE INFO

Received: 18 Nov 2024

Revised: 24 Dec 2024

Accepted: 18 Jan 2025

ABSTRACT

In the last ten years, cyber-attacks have become more advanced and frequent, creating danger for individuals, companies, and state agencies also. The main objective of this research paper is to evaluate various types of cyber threats such as ransomware, phishing attacks, DDoS attacks, APTs, and new emerging threats like "Digital Arrest". Now, let's looks into the societal and economic impacts of these attacks and presents practical measures that can be implemented to strengthen cybersecurity. The paper presents an approach towards protecting digital environments that takes into consideration the legacy and new emerging vulnerabilities.

Keywords: Digital Arrest, Cyber Attacks, Data Analysis, Trends, Attack Vectors, Threat Evolution

1. INTRODUCTION

The quick advancement of digital technologies has changed global operations, redesigned industries and enabling extraordinary connectivity in the world. With over 70% of transactions now directed online using the internet, the main motive of robust cybersecurity measures has never been greater. However, this technological evolution has also opened new paths for cybercriminals to exploit vulnerabilities which pose a significant threat globally.

Highly effective cyber incidents, such as the 2017 WannaCry ransomware attack, which affected over 150 countries [5], and the 2020 SolarWinds breach, which compromised US government agencies and Fortune 500 companies [6], highlight the critical need for broad cyber-attack defences to save the world from them. The implementation of legislation such as the EU's GDPR in 2018 [3] has helped to set stringent data protection standards; yet, the ever-changing cyber threat landscape necessitates more than legislative compliance to strengthen them.

This article investigates the challenges of modern cyber threats, examining their economic and societal consequences and suggesting effective solutions to combat them. We hope to provide a broad knowledge of the difficulties ahead by analysing previous instances and emerging concerns.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. TYPES AND EVOLUTION OF CYBER THREATS

With the development of technology and the global proliferation of networked systems, cybercrime rates have grown exponentially over the years. Over time, attackers have adapted their skills to include the more basic forms of cybercrime such as 'phishing' or more advanced tactics such as APTs (Advanced Persistent Threats). This section aims at the most important and rising threats of a cyber-attack and its categorization.

2.1 Types of Cyber Attacks

Individuals, corporations, and even nations are subjects of multiple different kinds of cyber-attacks. Below in a table is a general overview of the general types of attacks that happen around the world:

Table 1. Various types of cyber attacks

Type of Cyber Attack	Description	Examples	References
Phishing	Exploiting human vulnerabilities to steal credentials and sensitive information	COVID-19 Phishing Scams	[1, 2]
Ransomware	Malicious software that encrypts data until a ransom is paid	WannaCry, Colonial Pipeline	[5, 7]
DDoS	Overwhelming a service with traffic to disrupt operations	Russian-Ukrainian Conflict Attacks	[13]
Data Breaches	Unauthorized access to sensitive data	Equifax Breach	[2, 10]
Advanced Persistent Threats	Stealthy, long-term attacks targeting high-value information	SolarWinds Attack	[6, 11]
Supply Chain Attacks	Exploiting third-party software vulnerabilities	Kaseya Ransomware Attack	[11]
IoT Exploits	Targeting weak security in Internet of Things devices	Botnets, Device Hijacking	[9, 14]

Every type of attack has its own distinct form of complications. For instance, ransomware has a tendency to result in losses and the inability to access or retrieve information while APTs target and focus on long term persistent monitoring which makes it difficult to detect them. The severity of such problems is illustrated by the SolarWinds breach. Adversaries were able to carry out these attacks by exploiting the supply chain in order to infiltrate important systems.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

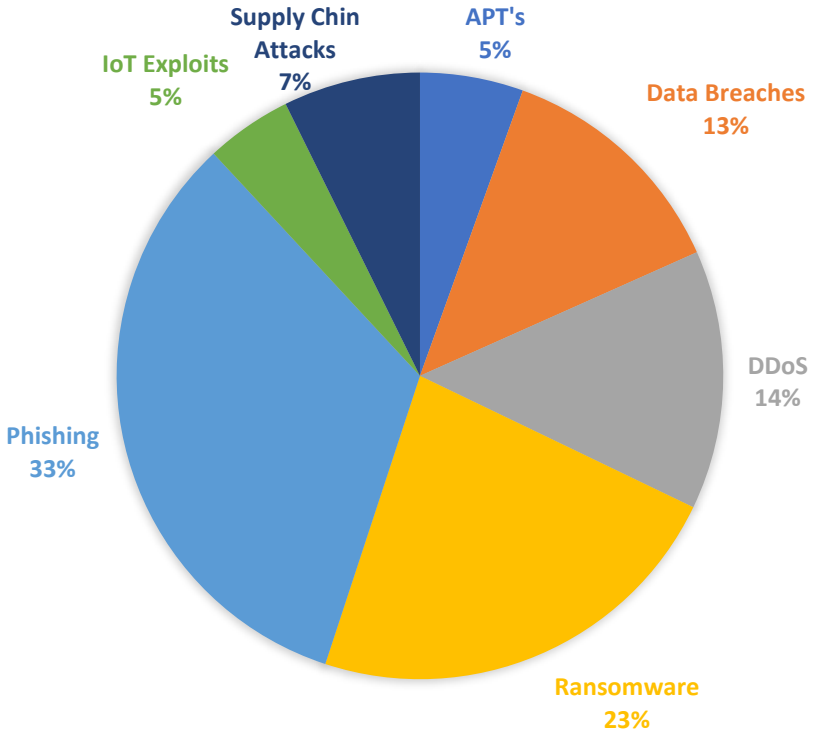

Fig. 1. *Distribution of cyber attacks*

2.2 New Threats

Clearly, as time goes by and new inventions are made, so are the threats out there. New cyber risks take advantage of innovation in tools such as AI and quantum computing. In the page following are some of these threats presented in summary form in a table.

Table 2. Emerging Cyber Threats and their impact.

Emerging Threat	Description	Impact	References
AI and Machine Learning Exploits	Manipulation of AI models to generate harmful outcomes	Misleading AI predictions	[12]
Quantum Computing Threats	Potential to break traditional encryption with quantum algorithms	Decryption of sensitive information	[16]
IoT Vulnerabilities	Exploits targeting weak Bluetooth and Wi-Fi security	Data Breaches, Device Hijacking	[9]
Digital Arrest	AI-driven attack combining social engineering and sophisticated tools	Disruption in healthcare, finance	[15]

These emerging threats highlight the need for proactive research and development of countermeasures. For instance, preparing for quantum computing's impact on encryption is crucial to safeguarding data.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

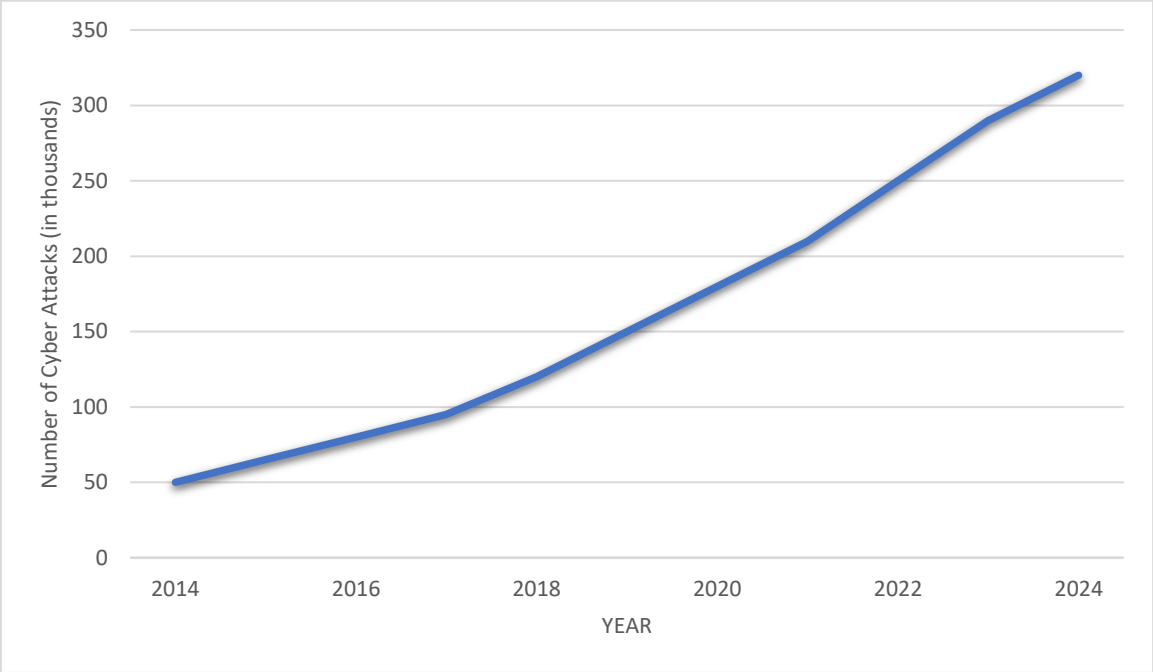

Fig.2. *Rise of Cyber Attacks in Last Decade*

3. IMPACT OF CYBER THREATS

Data breaches are a good example of incidents that reach severity levels from one to five. From robbing funds, to sabotaging one's financial standing, working a country's citizens mentality and crushing their puzzles of trust, and even damaging national safety for a country, a ussiano's analysis magnifies cyber incidences, their sequences, tendencies, along with the social impact and economic weight for each particular data breach version.

3.1 Historical Comparison of Cyber Threats

One of the most debilitating cyber-attacks, NotPetya, is estimated to have cost over $10 billion in damages across the globe, affecting multiple business and government entities. In terms of severity, Brookings Institution speaks of how this incident changed the market for cyber insurance because state-sponsored cyberattacks at this level required the redefining of coverage limits and damages insured.

Table 3. Most Famous Attacks, there types and impact on society

Year	Notable Cyber Attack	Attack Type	Impact
2013	Target Data Breach	Data Breach	$162 Million Loss
2017	WannaCry	Ransomware	$4 Billion Loss
2020	SolarWinds	Supply Chain Attack	Wide Government Impact
2021	Colonial Pipeline	Ransomware	$5 Million Ransom Paid
2022	Russian-Ukraine DDoS Attacks	DDoS	Govt & Financial Disruption
2023	Kaseya Ransomware	Ransomware	$70 Million Demanded

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Columbia SIPA's study NotPetya: The Evolution of Cyber Warfare suggests [27] that logistics and shipping automation reliant supply chains were affected the most. This also speaks to the more complex secondary effects of cyber danger, which goes beyond just immediate expenditures.

3.2 Economic Impact

The economic impact of cyber threats serves as an example for industries. The Colonial Pipeline was held ransom by a cyber-attack which shut down the fuel supply to the Eastern United States. SecurIT [29] analyzed this event and came to the conclusion that the entire economic impact, besides the ransom, which was $5 million, and the indirect economic loss due to fuel shortages and multiple businesses coming to a halt was over $100 million.

Table 4. Economical loss due to the attacks.

Attack Name	Year	Sector Impacted	Estimated Loss (USD)	References
WannaCry	2017	Healthcare, Business, Govt	$4 Billion	[5]
Colonial Pipeline	2021	Energy Infrastructure	$5 Million (Ransom Paid)	[7]
Equifax Data Breach	2017	Financial	$700 Million (Settlements)	[2, 10]
SolarWinds	2020	Govt, Fortune 500 Companies	Unquantified (Wide Impact)	[6]
Target Data Breach	2013	Retail	$162 Million	[18]
Russian-Ukraine DDoS	2022	Government, Financial	Unquantified	[13]
Kaseya Ransomware	2021	IT Services	$70 Million (Demanded)	[11]
NotPetya	2017	Multiple Sectors	$10 Billion	[5]

Similarly, The Digital Arrest scam is now emerging as a new danger towards business finances. Their national cyber-crime report on Facebook, [28], mentions that awareness and education programs are highly effective in reducing the number of victims falling prey to these scams. These programs aim to stop cyber criminals from manipulating people to give up sensitive information trespassing legal boundaries.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

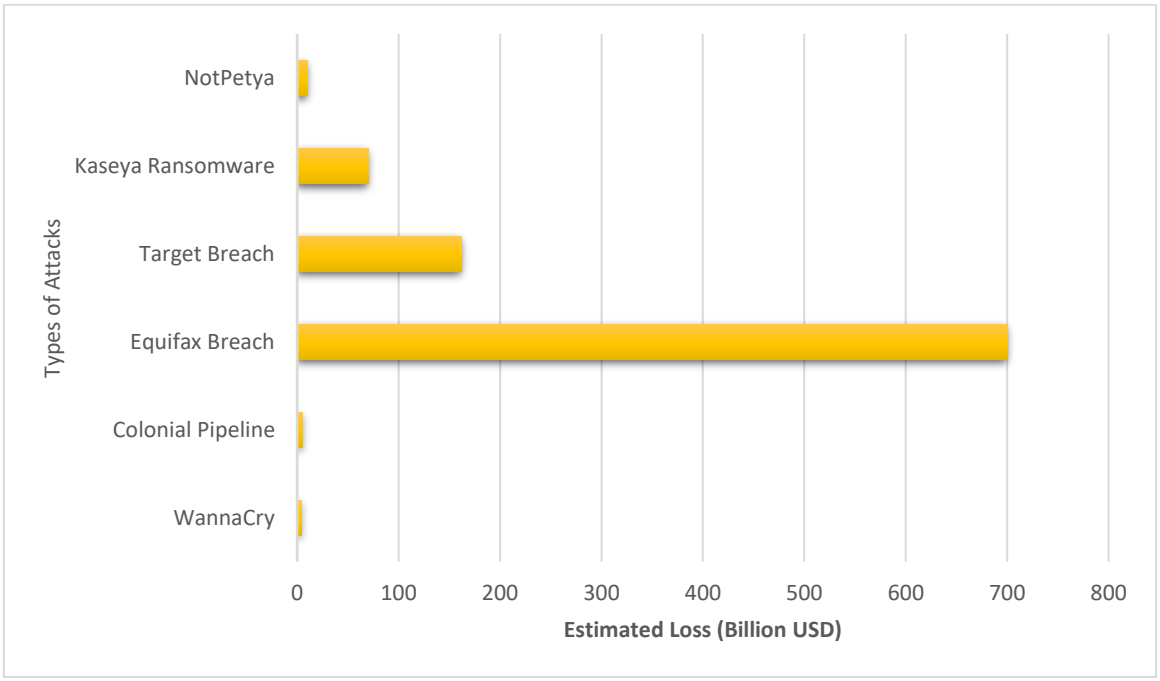

Fig. 3. *Economic Impact of Major Cyber Attacks*

4. SOLUTIONS AND RECOMMENDATIONS

Table 5. Possible solutions of the cyber-attacks.

Solution Category	Description	Examples	References
Public Awareness Campaigns	Educating individuals on identifying and avoiding cyber threats	Workshops, Media Campaigns	[9]
Advanced Technologies	Deploying AI-driven threat detection and quantum-resistant encryption	AI Tools, Quantum Encryption	[16]
Incident Response Plans	Regularly updated strategies for mitigating breaches	Cybersecurity Drills	[13]
Information Sharing	Promoting public-private partnerships to exchange threat intelligence	CERTs, ISACs	[12]
Regulatory Measures	Enforcing stricter penalties and fostering international cooperation to combat cybercrime	GDPR, US Cybersecurity Framework	[3]
Firmware Updates	Ensuring timely patches to address known vulnerabilities	Automated Updates	[14]

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhanced Encryption Standards	Protecting data transmission with robust protocols	AES-256, End-to-End Encryption	[9]
User Education	Empowering users with knowledge on safe IoT practices	Online Security Training	[10]

5. FUTURE DIRECTIONS

The emergence of technologies like AI and quantum computing creates many events in the world of cybersecurity. From our review, exploring quantum resistant cryptography and AI systems' anomaly detection are areas that warrant greater attention [16]. Addressing the digital arrest problem will also contribute to resolving challenges in creating flexible adaptive and self-evolving cybersecurity solutions [15].

5.1 The Role of Blockchain in Cybersecurity

Blockchain technology has great potential in addressing some of the challenges facing cybersecurity. Because the technology offers a single source of truth, it can be used to:

1. **Protect Supply Chains:** Information within supply chain systems cannot be altered [12].
2. **Identity Management:** Verification can take place without a governing body [10].
3. **IoT:** Controlled information dissemination can be established for IoT systems [14].
4.

Setting forth the novel technologies that should be set forth with blockchain will definitely help stakeholders to achieve enhanced cybersecurity in the coming years.

5.2 Digital Arrest Scam

The Digital Arrest scam is a multifaceted scheme that uses AI and deepfake technology to create very realistic impersonations of enforcement officers. Victims are compelled into providing private information, or making payments under the misconception that they are being legally investigated. According to Facebook Cybersecurity Initiatives [28], these campaigns have helped raise public awareness of these threats, which in turn has reduced the number of victims and made these types of scams less effective.

Key Phases of a Digital Arrest Scam:

1. **Initial Contact:** Attackers pose as officials from legal authorities using spoofed emails or calls.
2. **Fear Tactics:** Victims are threatened with legal consequences to create panic.
3. **Data Extraction:** Under pressure, victims provide sensitive information.
4. **Monetary Extortion:** In some cases, attackers demand ransom to avoid supposed legal action.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

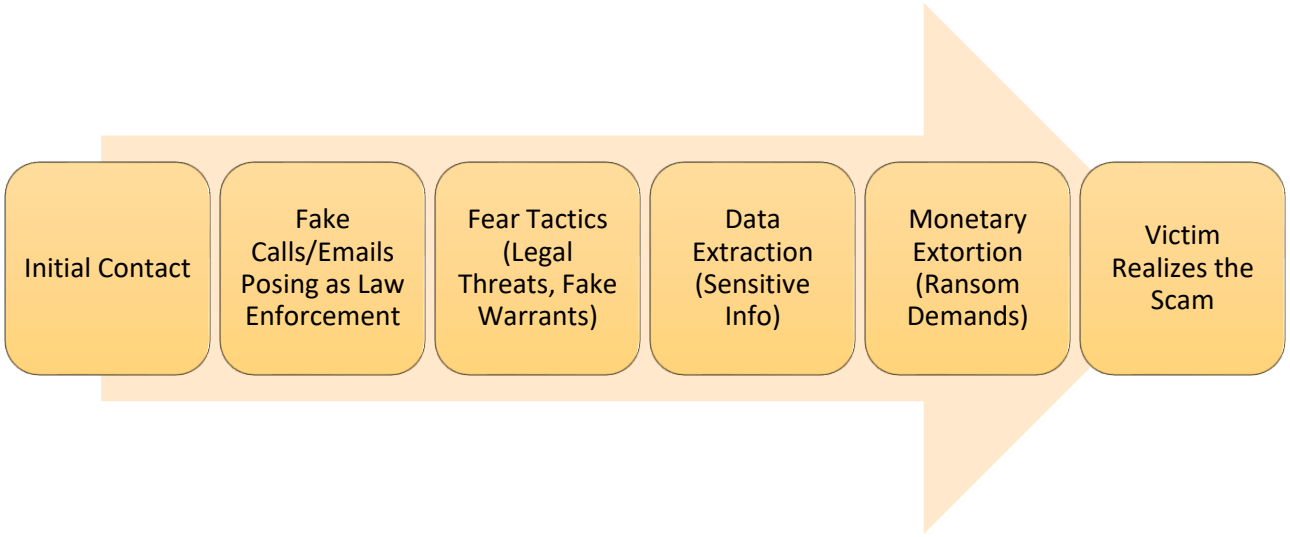

Fig. 4. *Process Flow of a Digital Arrest Cyber Scam*

6. CONCLUSION

The evolution of cybercrime elevates the importance of cybersecurity to new heights. The past decade saw severe breaches such as WannaCry, SolarWinds, or the Colonial Pipeline Ransomware which cost financial, confidential, and even national security. New emerging threats such as AI attacks, quantum computing, and Digital Arrest cyber scams are all signs of new technologies being employed by criminals to exploit the everchanging face of technology.

A multi-pronged tactic is necessary to take on these problems. Newer technologies such as AI based attacks detection, stronger encryption, and systems utilizing blockchain are a good start, but they are not enough. Policies need to be targeted at governments, businesses, and cybersecurity practitioners to mitigate online safety issues through awareness and education.

At the same time, these policies need to take into consideration that cybersecurity threats will keep changing. Individuals and organizations should continue learning and adapting to newer protective measures such as system updates, user education, and regular threat surveillance. By doing so, we greatly mitigate risk. Remaining vigilant and stakeholder cooperation is key to a safer technological world.

REFERENCES

1. Verizon. 2023. "Data Breach Investigations Report." Verizon Communications Inc.
2. IBM. 2023. "Cost of a Data Breach Report." IBM Security.
3. European Union. 2018. "General Data Protection Regulation (GDPR)." Official Journal of the European Union.
4. Bhardwaj, Akashdeep, Salil Bharany, Anas W. Abulfaraj, Ashraf Osman Ibrahim, and Wamda Nagmeldin. 2024. "Fortifying Home IoT Security: A Framework for Comprehensive Examination of Vulnerabilities and Intrusion Detection Strategies for Smart Cities." Egyptian Informatics Journal 25. doi: 10.1016/j.eij.2024.100443.
5. WannaCry. 2017. "Ransomware Case Study." Cybersecurity Ventures.
6. SolarWinds. 2020. "Supply Chain Attack Report." SolarWinds Corporation.
7. Colonial Pipeline. 2021. "Ransomware Analysis." Colonial Pipeline Company.
8. Cook, S., et al. 2024. "Bluetooth Vulnerabilities in IoT Devices." Journal of Network Security 34. doi: 10.1016/j.jns.2024.100512.
9. Yaacoub, J., et al. 2023. "Ethical Hacking for IoT Security." International Journal of Cybersecurity 21. doi: 10.1016/j.ijc.2023.100467.

10. Symantec. 2022. "Cyber Threat Analysis." NortonLifeLock Inc.
11. FireEye. 2023. "APT Report." Mandiant Intelligence.
12. Rachakonda, L., et al. 2024. "Cybersecurity Challenges in 5G Networks." Journal of Communication Networks 29. doi: 10.1016/j.jcn.2024.100522.
13. World Economic Forum. 2023. "Global Risk Report." World Economic Forum Publications.
14. Schiller, E., et al. 2022. "IoT Security Landscape." Journal of Information Security 18. doi: 10.1016/j.jis.2022.100389.
15. Rudrakar, S., et al. 2023. "IoT in Agriculture: Security Challenges." Agricultural Informatics Journal 12. doi: 10.1016/j.aij.2023.100402.
16. IBM X-Force. 2023. "Threat Intelligence Index." IBM Corporation.
17. Sadikin, F., et al. 2023. "Penetration Testing for ZigBee Systems." Journal of Wireless Networks 28. doi: 10.1016/j.jwn.2023.100533.
18. Ai, M., et al. 2022. "Blacktooth: Exploiting Bluetooth Vulnerabilities." Journal of Network Security 20. doi: 10.1016/j.jns.2022.100459.
19. Infosecurity Europe. 2023. "Learnings from the NotPetya Cyberattack." Infosecurity Europe Reports.
20. Reuters. 2024. "Vardhman Group Chairman Scammed in Digital Arrest Scam." Reuters News Agency.
21. Brookings Institution. 2023. "The Economic Impact of Cyber Insurance after NotPetya." Brookings Cybersecurity Studies.
22. Columbia SIPA. 2023. "The Global Effects of NotPetya." Columbia University School of International and Public Affairs.
23. Facebook National Cyber Crime Reporting. 2024. "Digital Arrest Awareness Campaign." Facebook Cybersecurity Initiatives.
24. SecurIT. 2024. "Analyzing the Colonial Pipeline Ransomware." SecurIT Research Publications.
25. Cybersecurity Ventures. 2023. "Global Ransomware Damages Predicted to Hit $265 Billion by 2031." Cybersecurity Ventures Reports.
26. Abidin, Shafiqul,.Vadi, VR,. Rana, Ankur, October, 2019. On Confidentiality, Integrity, Authenticity and Freshness (CIAF) in WSN: 4th Springer International Conference on Computer, Communication and Computational Sciences (IC4S 2019), Bangkok, Thailand. Publication in Advances in Intelligent Systems and Computing pp 87-97, ISSN: 2194-5357.
27. Ayasha Malik, Veena Parihar, Jaya Srivastava, Shafiqul Abidin, “Necessity and Role of Blockchain Technology in the Domain of Cyber Security and Data Science”, International Conference on Computing for Sustainable Global Development (INDIACom), I**EEE *Xplore,*** May 2023.
28. Ayasha Malik, VeenaParihar, Ja Srivastava, Harpreet Kaur, Shafiqul Abidin, “Prognosis of Diabetes Mellitus Based on Machine Learning Algorithms”, International Conference on Computing for Sustainable Global Development (INDIACom), I**EEE *Xplore,*** May 2023.
29. Vadi, VR., Abidin, Shafiqul., Khan, Azimuddin., Izhar, Mohd. August, 2022. Enhanced Elman spike neural network fostered blockchain framework espoused intrusion detection for securingInternet of Things network: Transactions on Emerging Telecommunications Technologies, John Wiley, ISSN:2161-3915.