Page 407 - 425 **DOI:** *https://doij.org/10.10000/IJLSI.111900*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

The Growing Necessity of Cybersecurity and, in the End, Defending against Cyber Threats and Dangers

MANTASHA AFAQUE FAROOQUI[1] AND ANCHAL RANI SINGH[2]

ABSTRACT

In an era where digital technologies are vast, the notion of cybersecurity has become important to the security and integrity of our connected environments. This essence provides an elaborate oversight of the intricate domain of cybersecurity in the digital sector, sketching the main issue, solutions and difficulties related to safety our digital assets. The term "digital domain" denotes to a broad range of circumstances, including personal electronics, corporate networks, critical infrastructure, and the Internet in common. The Internet of Things (IoT) has developed several opportunities, but it has also made new attack vectors and weaknesses that can endangered the availability, secrecy, and integrity of linked systems. A systematic and detailedperspective to find out and to reduceprobability security weaknesses is crucial in the growth of a protected Internet of Things ecosystem. Ideas related to cybersecurity research are crucial in the sense that they serve as a basis for making and executing security solutions that can deal with new threats. The digital domain covers a broad range of references, including personal gadgets, business networks, critical infrastructure, and the Internet as a whole. The essence looks at how the threat landscape is changing and covers a broad range of cyber threats, from intricate nation-state-sponsored steerage to malware and phishing attacks. The enhanced number of cyber-attacks poses a grave threat to financial institutions, public safety and national security, in addition to weaknesses data privacy and secrecy. Progressing such requirements requires an interdisciplinary team attempt with multiple stakeholders, involving domain experts, network architects, system designers, and cybersecurity experts. The complexity web of internet platforms and applications in the digital marketing industry makes cyberattacks especiallyoften. A hacked website or tempered with online impedance can cause operations to be obstructed, trust to be lost, and brand reputation to be cause harm. A number of contrivance and technologies are used to reducethis intimidation, from machine learning-based inconsistencytrace and artificial intelligence to firewalls and antivirus programs. Besides, strong policies, employee training, and incident reactionprocess are part of a detailed cybersecurity program that goes ahead technical

[1] Author is a student at Integral University Lucknow, India.
[2] Author is a LL.M. student at National University of Research and Study in Law, Ranchi, India.

 [ISSN 2581-9453]

security steps. Together with the digital sector, cyber security should also move ahead. The Internet of Things (IoT) and quantum computing are two new technologies that come with their security anxiety in the abstract. It also insists how crucial international cooperation and regulation are becoming in the pursuit of a safer digital environment. The abstract thrown light on the fact that cyber security is a vast and movingdomain in the digital sphere. Given the moving and intricate nature of cyber threats, it is crucial for individuals, corporations, and government entities to be alert and flexible. A detailed plan that unified technology, law and human understanding is crucial to effectively protect our digital future.

Keywords: *Cybersecurity, Cyberthreats, Digital Domain, Internet of Thing (IOT).*

I. INTRODUCTION

"If it is known, its manageable. If it's well-known, it's actionable". - Bradley B Dalina

We live in a time of unprecedented innovation, communication and business due to the evolution of digital technology and the globalization of society. As a result of this digital progress as well as the concerningenhancement in cybercrime, societies around the world are facing a difficult and complex task.Recognizing the basis of cybersecurity is the idea that everyone uses cyberspace, a collective term for all online and electronic platforms, as targets for cybercriminals. Denoted objects can include our money or data, as well as things like documents, emails, Internet presence, usernames and passwords.While denoted attacks occasionally occur, most cyberattacks are usually and can affect anyone. Anelemental and often driver of cyberattacks is human error. These conveniences range from as simple as trusting indication delivered electronically in phishing emails to thieves pretending to be customers, suppliers, or even staff members or experts in order to access your assets (financial and otherwise). So, computer security is need to safeguard against these attacks.[3]The rate of cybercrime has risen in our country due to the expansion of mobile and high-speed internet. People may be tendered advise not to travel to remote locations where thieves can rapidly take items and ran away to the offline world.But the digital world is a totally different place, and even an educated person can become a victim of cybercrime. India is particularly unsafe to the threats posed by cyber criminals as it has one of the biggest and fastest growing digital populations in the world. Identity theft, cyber terrorism, financial fraud and data breaches are just a few examples of the complex and ever-emerging scope of cybercrime.India's digital changeIt is the culmination of varioustechnicaloutcome and breakthroughs. Most people in

[3]Dario Rodriguez, Information Technology Within Society's Evolution, 40 Technology in Society (2015).

India do not always have access to computers, the Internet or other devices that are commonly used to access social media websites such as Facebook, WhatsApp, Skype, chat rooms and dating services. on one hand, digitalization has developed India's system in every way, including governance, economics and education. Nevertheless, this led to a crucial increase in cybercrime in India.[4]Crime is a social and economic event as old as history and human civilization. Mainly Crime is a notion and a legal liability. A mistake in law that could affects in criminal charges and possible fines is known as a crime or misdemeanor. Crime, in all its forms, always effect society, directly or indirectly.Computer security, as it connects to IT and computing, involves safeguarding and powerful computing resources, data integrity, inhibit unauthorized activity, preventing enemy people from accessing the system, and above all maintaining and implementing data privacy.Since malicious devastation, illegal unveiling, or unwarranted access by users or entities are all possible, any system meeting security criteria must keep its resources available for legal access and use in a timely and constantmeans. To maintain its integrity, availability and confidentiality, the automated system must be kept secure.[5] It is said that every person who uses the Internet leaves a digital mark of his or her identity and personal information. We have fraudsters and cybercriminals discover new ways to thieve people's personal information, and few of the online activities we participate in are not safe.[6]

Cybersecurity is greatly influenced by the Internet of Things (IoT), which has become a crucial technology in today's world. IoT devices are subject to several cyber threats due to their broad reach use, interconnectedness, and often lack of critical security measures. Attackers using distributed denial of service (DDoS) methods can exploit these vulnerabilities to gain sensitive data and even take over censorial infrastructure. A large-scale cyberattack on IoT networks can have serious outcome, such as dissolution of critical services and vital financial losses.The complicated network of people and things is known as the Internet of Things work together to share and monitor data about Usage as well as environment strength smart devices with CPUs, sensors, and networking gear, systems are capable to collect, transmit, and store dataprocess data from their environment as part of the Internet of Things ecosystem. To share sensor data with each other, these IoT gateways or other edge equipment are connected to IoT devices.After processing locally, the data is moved to the cloud for analysis. These devices

[4]Sanjeev Kumar, Cyber Crime Against Women: Right to Privacy and Other Issues, 5 The Law Brigade (Publishing) Group (2019).
[5]Sabina Lissitsa, Effects of Digital Use on Trust in Political Institutions Among Ethnic Minority and Hegemonic Group -a Case Study, 66 Technology in Society (2021).
[6]John Mason, 5 Cybersecurity Challenges and Trends: What to Expect in 2018, GlobalSign Blog (Jan. 10, 2018), https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018.

communicate with each other on a daily basis and work in pursuance to each other's feedback. Internet of Things devices frequently operate on their own, without human aid. The Internet of Things is a quickly growing field, with connection to device interoperability, data privacy, and security.People who use IoT not only have more command over their lives, but they can also live and work more emphatic way. IoT technology bestowdevices that businesses can use to automate enterprise environments, so businesses keep faith on it firmly. In addition, the Internet of Things decreases production and shipping costs, reforms service efficiency and bestowed visibility into corporate processes. Prepackaged Software as a Service (SaaS) solutions, or intelligent Internet of Things (IoT) apps, use machine learning to calculatelarge scale amounts of data collected from network sensors and bestow useful insights to business users via an interface furnished with algorithms.Securing the Internet of Things is one of the chiefdefiance it presents. These devicesgather private information like your words and actions at work and home. The reliability of the Internet of Things is crucial to users' trust in it, yet data security is one area where it falls short. Due to unfair management of user and device data during storage and transmission, many linked systems fail to bestow a suitable level of security.[7]

(A) Meaning of cybersecurity

Cybersecurity comes into play due to the existence of number of cybercrimes just like there are laws and punishment because them exists the law breakers and criminals same as there is concept of cybersecurity due to existence of cybercrimes. To know cybersecurity we need to know cybercrimes first and that could be defined as every crime that takes place over the internet by use of computer devices and network or can be described as illegal and unauthorized access to computer systems with malice intention in order to harm an individual, group of people, any private organization or against government whereas cybersecurity can be described as a process of protecting computer systems, digital data and networks from damage ,theft , unauthorized access and any other kind of cyber threats.It is a process by which data information that circulates over the internet between group of people all over the world are secured and protected from unauthorized, dirty use, exploitation and alteration of devices. It also incorporates different tools and techniques of safeguarding computer networks, data and programs from unauthorized attacks and access which may result in any kind of damage to computer systems and data so circulated. A worthy and good cybersecurity diagnoses all the threats and vulnerabilities a network or computer system could have and protect them from

[7]Ajeet Das & Olga Yashkova, Market Analysis Perspective: Worldwide Internet of Things, 2022 — Infrastructure and the Intelligent Edge, The Premier Global Market Intelligence Company. https://www.idc.com/getdoc.jsp?containerId=US49735922.

such threats and damages that incurred to it without much time fixes all these vulnerabilities effectively and efficiently.[8]

II. HISTORY OF CYBER SECURITY

Despite what the general public may reckon, the field of cybersecurity is not relatively new. You would be wrong to reckon that the origins of cybersecurity can be traced back to the earliest instance of computers connecting to the Internet, because cybersecurity also includesafeguarding data that used to live only on computers, not on any network.Digital threats were rare in the beginning days of computers, often limited to distinct cases of simple malware and computer viruses. But the landscape of digital threats transformed dramatically in the 1990s as technology developed and the Internet became broadly used. Due to the progress of Internet communications and linked systems, rogue actors now have even more ways to exploit weakness.Threats that were more developed, including Trojan horses and worms, began to appear in the late 20th century and diffusequickly through networks. With the enhance in cybercrime in the new century, botnets have become more and more extensively for large-scale attacks. The aims of threats to the digital areasecede, ranging from financial gain to political and ideological, as society becomes more and more dependent on digital infrastructure.State-sponsored cyberattacks became more general in the 21st century, making the digital threat picture more complicated. The increase in ransomware attacks, data breaches, and cyber spying has had a nationwideinfluence on corporations, governments, and individuals. With the continualprogress of technology, a dynamic and ever-changing environment has been built by the perfection of cyber criminals to safeguard digital assets.[9]

(A) Need of cybersecurity in today's context

we are living in the era where we are totally dependent on the machines, digital world and most importantly on the Internet:A gift by a human to another human.Today, the entire world and it's working is carried out by networking system and the internet besides it is one of the best creation of human sadly it has dark sides too. Sadly, there are number of characteristics that makes internet the best tool to explore at the same time this tool is used in abrupt manner and resulting in number of cyberattacks against government, an individual,a group of people or any private organization. This gave rise to the need of cybersecurity as cyberattacks and its threats is increasing day by day. According to the recent reports it was find that more than 700,000

[8]Cyber Crime & Cyber Security, https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm.
[9]Vikki Davies, The history of cybersecurity, Cyber Magazine, (Oct. 4, 2021), https://cybermagazine.com/cyber-security/history-cybersecurity.

people every year falls prey of these cyber attackers and become their victims. Therefore, protecting and defending entire World from these cyberattacks had become a huge concern as it has the capability to cause damage to millions of people,hamper a happy living family, and most tragically can result in the shutdown of any state-ownedorganizations. This can be illustrated with an example of city of Atlanta which was attack by the known ransomware Sam the hackers have demanded huge amount that was about $51 million and threat was this much malicious that in order to stop it the internet service of the city was disconnected for almost 5 days and the city however managed to get rid from these attackers after paying $17 million to them.

As explained in the research that took place at Brooking institution, it was pinned that due to the advancement in the technology and introduction of 5G networks there is an increment in the vulnerability of multi-dimensional cyberattackers.Due to increase in modern technologies like internet of things(IOT) that has resulted in landmark increment in variety of devices connected and linked to the internet that has made easier for the cyber criminals to have access to such devices and they can effortlessly enters into the computer systems without any human help .For the purpose of safeguarding data, personal information as well as protecting business activities, confidential information we need cybersecurity to work efficiently at the large scale with increasing awareness regarding these cyberattacks And cyberthreats.[10]

(B) The importance of cybersecurity in the digital space

To guarantee the sustained use of sensitive data in cyberspace, governments and societies around the nations must place anexalted premium on data security. It is important to use cybersecurity on an individual basis to safeguard one's personal information, such as images, documents, videos, passwords, bank account information, and personal accounts. To safeguard society from social engineering and target social behavior, we collected data and maintained community privacy at the community level.[11] Concerning the security of electronic resources, information and data (such as personnel data), servers and websites within corporate settings and within separate business categories. As well as safeguarding the state's radio, television and military networks against electronic attacks, theft, etc. dissolution, it also safeguards the state's electronic security.[12]

[10]Diva Rai, Cyber Crime and Cyber Security: An overview, IPleaders (Nov. 13, 2019), https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/.
[11]Renas R Asaad, Penetration Testing: Wireless Network Attacks Method on Kali Linux OS, 10 Academic Journal of Nawroz University 7-12 (2021).
[12]Mohammed Ahmed Jubair & Salama A Mostafa, A QoS Aware Cluster Head Selection and Hybrid Cryptography Routing Protocol for Enhancing Efficiency and Security of VANETs, 10 IEEE 124792-124804 (2022).

It is impossible to underestimate the contingency of cybersecurity in the digital area. Cybersecurity is crucial in today's connected world for several reasons, as nearly every part of our lives depends on digital technology:

- **Security of Personal Data**: In the digital era, a many personal data is kept online, including financial, corporate and personal data. Cyber security ascertains the security and privacy of people and organizations by inhibiting illegal access, theft or amendment of this data.
- **Preventing Data Breaches:** Financial losses, harms to one's prestige, and legal outcomes are some of the serious influences that can result from data breaches. To stop these attacks and maintain the trust of stakeholders and consumers, effective cyber security steps are critical.
- **Security of Critical Infrastructure**: As digital technology becomes more and more identical to fragile infrastructure, such as power grids, transportation networks and health care facilities, its crucial is increasing. Cybersecurity is crucial for both national security and public safety because cyberattacks on this arrangement have the potential to have real-world impacts.
- **Fighting Cyber Crime**: Hackers are continuously changing their strategies to take benefits of vulnerabilities in digital systems. Strong cybersecurity safety is necessity to discern and haunt hackers, as well as safeguard against threats such as ransomware, malware, and phishing scams.
- **Maintaining Confidence in Virtual Trading**: Virtual trading and virtual currency swap have become an important part of synchronous existence. In the deficiency of strong cybersecurity, consumers may be indisposed to transact online, which will hinder innovation and economic progress.[13]

(C) Benefits of cybersecurity

In today's age, everyone get advantage from using advanced software to safeguard against cyberattacks. In fact, a person can experience a diversity of unpleasant outcomes from a cybersecurity threat, including devastation of identity documents, extortion attempts, and theft of personal information such as family photos.Ahead, institutions such as power plants, hospitals, and financial services companies are necessary to everyone's daily survival, thus their security is important to guarantee the suitable functioning of society. Nowadays, adopting

[13]Dinesh Kumar Saini & Jabar H Yousif, Vulnerability and Attack Detection Techniques 10 (1st ed. 2021).

contemporary cyber security software can be profitable for anyone.They want to encourage open-source software toolkits, draw attention to recently discovered vulnerabilities, and notify the broader public about the significance of cybersecurity.[14]

It is crucial to safeguards society from cyber-attacks because, if they happened, the damage could harm millions of people, force state-run businesses to close, and devoid citizens of access to services.Cyberattacks using ransomware can take placenationwide, and as hackers gain access to government institutions, it is crucial to bestow the fieldwork for future defense against cyber-attacks on feeble infrastructure like power grids and factories. Cyber-attacks could take place on nuclear power plants, causing destructive destruction and the deaths of millions of people.Five centrifuges are decimated in an attack on an Iranian nuclear site by anenemy computer virus. Due to the spread of these electronic viruses, several people may die in explosions caused by overheating of centrifuges.[15]

In pursuance to research from the Brookings Institution, rapid technological progress resulting in the deployment of 5G networks could expose consumers to extensively and multifaceted cyberattack risks. Cyber criminals can now use artificial intelligence and machine learning to launch cyberattacks due to the extensively adoption of contemporary technologies such as The Internet of Things has resulted in a crucialrise in the number of gadgets with Internet connections. An application which is competent of easily breaking into a computer system without the requirement for human interference. There is thinkable concern about these automated cyberattacks because they have the potential to be carried out on a global scale.[16]In an effort to secure commercial enterprises, cyberattacks aiming these businesses have increased in recent years, resulting in losses and millions of dollars spent in restoring their data. All these accusations will not only force executives out of their jobs, but may also cause the company to cut costs, resulting in layoffs of other employees.These companies include the credit bureaus, a financial services company, Yahoo, a giant online company whose data breach influenced all 3 billion of its accounts, and Target, a store whose data breach impactedseveral customers and for which the cost of recovery reportedly was estimated to be $1 billion global credit rating agency, which had to face unauthorized access that influencedmany customers and whose recovery cost was recently estimated at $439 million. An estimated $350 million has been directly invested in the restoration project.[17]

[14]Zina Balani & Hacer Varol, Cloud Computing Security Challenges and Threats, IEEE 1-4 (2020).
[15]Fariba Ghaffari & Hossein Gharaee, Cloud Security Issues Based on People, Process and Technology Model: A Survey, IEEE 196-202 (2019).
[16]Zina Balani & Hacer Varol, Cloud Computing Security Challenges and Threats, IEEE 1-4 (2020).
[17]Supra Note 11

III. INTERNET OF THINGS, COMMON ARCHITECTURE, COMPONENTS AND PROTOCOLS FOR THE INTERNET OF THINGS

The dictum "Internet of Things" (IoT) refers to a network of original physical objects, such as vehicles, devices, and other objects, that are related to the Internet, have sensors, and other information to facilitate sharing and collecting data. Are unified by software.This equipment, generally referred to as "smart objects", can range from simple "smart home" devices like a thermostat, to wearable technology like a smartwatch and apparel with RFID capabilities, to intricate transportation and industrial networks. Technologists are also speculating on "smart cities" consisting of holistic IoT.

With the help of the Internet of Things (IoT), this smart equipment can communicate with portal and smartphones, in addition to other Internet-enabled devices, to establish a huge network of interconnected devices that can exchange data and can enactseveral types of tasks on your devices. This can include everything from tracking the weather on farms, controlling traffic patterns using smart cars and other smart automotive devices, leading machinery and procedures in factories, and keeping track of shipments and inventory in warehouses.IoT equipment are used in enterprise settings to monitor severalfeatures including machine display, energy usufruct, temperature, humidity, and air quality. By using real-time data analysis to find patterns, trends and discrepancy, businesses can customize their operations and increase their income.[18]Albeit there is no pre-planned blueprint for Internet of Things Network, application, and inspection are three separate but connected levels that make up the design. But digital communications giant Cisco went one step further and established a total of seven levels.[19]

First, physical equipment; Second, Exchange and management of information lastly, transformation and analysis of data; Fourth, storage of data; Fifth, abstraction and grouping of data; And sixth, application. Furthermore, seventh, participation and commerce. procedure were the layers that CISCO specified. We focused on security vulnerabilities influencing the network, application, and observation layers. According to multilayer security technology, each essence of an IoT cybersecurity strategy should have backups to cover any flaws or shortcomings. These layers work together to strengthen a company's safety and lay the base for a successful Internet of Things (IoT) cybersecurity strategy. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is established on primary functions including Identify, Protect, Detect, Respond, and Recover, is also explored.To model the

[18]What is the internet of things? | IBM, https://www.ibm.com/topics/internet-of-things. (Jan. 05, 2024)
[19]Denise Gregonis, https://www.cisco.com/c/dam/global/en_ph/assets/ciscoconnect/pdf/bigdata/jim_green_cisco_connect.pdf(Jan 05, 2024),

intimidation landscape for IoT security, we put the "tuple model" into practice. The model included the target, impact, attacker, and attack vector. The attack vector essence detailed the means or methodology by which the attack was carried out, while the attacker element directed the person or organization in charge of the attack. The IoT device or system that was the target of the attack was represented by the target essence, and the influence element explained any potential harm or outcome that could arise from the attack.The growth of a holistic threat model considering each landscape was facilitated by the tuple model, which offered a framework for identifying separate types of threats and vulnerabilities in Internet of Things systems. Thus, to detect more intricate threats – that is, attacks with various stages or threats involving various targets –, this model can be improved to include more features.

- **Observation Layer**

The observation layer is liable for receiving and exchanging data and is composed of various IoT sensors and other hardware elements. The Internet of Things depends on heavily on sensors and other technologies to trace and relay information. Intelligent wirelessly connected sensors that collect data form a wireless sensor network (WSN)about environmental circumstances. One or more relay stations transmit sensitive data to a central hub or base station.[20]

- **Network Layer**

The received data is stored by the network layer or forwarded to the application layer for further processing with the aid of inputs from the observation layer. This layer is most crucial in the context of the Internet of Things because it connects various types of communication technology that allows IoT devices to communicate with each other. Readable tags and Zigbee are two of the most broadly used of these communication technologies.[21]

IoT devices can be left unattended for long duration of time, have low capabilities and confined power sources. They also originate a lot of data. Thus, when progressing security measures, it is necessary to take into account the special characteristics of IoT devices. In contrast, various specifications and functionalities may apply to traditional wireless networks and devices. The exact execution and factors taken into account may secede for each form of network, even though some security notion may be similar.Both conventional wireless networks and the Internet of Things use separate protocols and norms. As picture,both use the IEEE 802.11 norms for wireless LANs and Transmission Control Protocol/Internet Protocol (TCP/IP) for

[20]ChunHua Cao &YaNa Tang, IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security, 1-8 Security and Communication Networks 2021 (2021).
[21]Mukhtar Ahmad Sofi, Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review, 5 International Journal of Engineering Research & Technology (IJERT) (2016).

communications. Besides this, both use data transmission security protocols including Transport Layer Security (TLS) and Wi-Fi Protected Access (WPA). Albeit, the protocols and norms employed by the two categories of networks secede in many other ways. For example, many Internets of Things devices use low-power, low-data-rate wireless technology.While high data rate protocols such as Long-Term Evolution (LTE) or WiMAX are generally used in classical wireless networks, Zigbee or Bluetooth Low Energy (BLE) are more common. Ahead, the kind of protocols and norms that can be employed are forced by the limited processing and memory capacity of IoT devices. For this reason, specific protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are frequently used in Internet of Things devices. For both local and remote landscape, specific needwas taken into account. These included hardware connectors, Internet of Things gateways, wireless device connectivity, and communication protocols.[22]

- **Application Layer**

The application layer keeps the keys to difference between Internet of Things devices and their communication networks. It acts as a helpful intermediary between the operation of an IoT device and the data transfer that happens over the network. The best protocol for each Internet of Things application depends on variouscause, including the type of device and the work it acts. Message Queuing Telemetry Transport (MQTT) and Constraint Application Protocol (CoAP).[23]Application protocols that are most generally used. Thanks to the progress of CoAP, low-power, low-resource devices can now relate to the Internet of Things across faint, unstable networks. Its main application is in M2M (machine-to-machine) systems, which permit machines to communicate with each other to perform activities such as smart lighting and HVAC (heating, ventilation and air conditioning) system metering and control. CoAP uses UDP (User Datagram Protocol) for information transfer. For data security, CoAP takes benefits of the authentication and encryption features of UDP. While HTTP (Hypertext Transfer Protocol) uses TLS over TCP (Transmission Control Protocol), CoAP datagrams over UDP use TLS (Transport Layer Security) (Rivest-Shamir-Adelman), or RSA.[24]Datagram Transport Layer Security (DTLS) assist a variety of ciphers, including Advanced Encryption Standard (AES).[25]

[22]Max Ingham &Deepayan Bhowmik, IoT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN, 14 IET Information Security (2020).
[23]Victor Seoane & Florina Almenares, Performance Evaluation of CoAP and MQTT With Security Support for IoT Environments, 197 The International Journal of Computer and Telecommunications Networking (2021).
[24]Sitalakshmi Venkatraman & Anthony Overmars, New Method of Prime Factorization-Based Attacks on RSA Authentication in IoT, 20 Cryptography (2020).
[25]Chung-Wen Hung & Wen-Ting Hsu, Power Consumption and Calculation Requirement Analysis of AES for

With its low resource claims and limited bandwidth, MQTT was designed as a simple publish/subscribe messaging system that is good for connecting distant devices. For wireless networks experiencing intermittent throughput spout or irregular connectivity, MQTT is a great choice due to its variable delay. The MQTT protocol with TLS security capacity can bestow a credible, lightweight, and emphatic bi-directional communication system between millions of devices.[26]

IV. INDIA'S REGULATORY FRAMEWORK

Post-pandemic, India's ever-expansion digital infrastructure has enhanced the demand for new, updated and enhanced regulatory mandates to secure cybersecurity. As per the IBM Security Data Breach Report 2022, the average cost of a data breach in India for fiscal year 2022 was ₹17.5 crore (₹175 million) or about $2.2 million. This represents a shocking increase of 25%. The average cost in 2020 was ₹14 crore and a rise of 6.6% from 2021.[27]

Current Legislations Regarding Cybersecurity Used in India are:

(A) National Cyber Security Policy, 2013

To establish "a safe and flexible cyberspace for citizens, businesses and government", the National Cyber Security Policy of India was formulated in 2013.[28]The strategy accepted the threats that cyberattacks pose to national security, to the economy, and human life. Besides, the policy identified vital cyberspace security strategies, most of which are still in use today. India's cyber atmosphere needs to be better guarded, and the National Cyber Security Policy target to do this by developing more dynamic policies. The policy intends to use skill development and training to prepare more than 500,000 skilled IT professionals over the next five years. Objective of NCSP was Establishing a protected and flexible online atmosphere for people, businesses and government and monitoring, protecting data and cyber infrastructure, decreasing weak points and strengthening defenses against cyberattacks and establishing structures, capabilities, and vulnerability management plans to more rapidly mitigate, prevent, or address cyberattacks and threats. Albeit, a new national cyber security policy is long overdue, as the current policy is ten years old. In December 2022, the government promulgate

WSN IoT, 18 Sensors (2018).
[26]Ángel Luis Muñoz Castañeda & José Antonio Aveleira Mata, Characterization of Threats in IoT from an MQTT Protocol-Oriented Dataset, 9 Springer Science and Business Media LLC (2023).
[27]Cost of a data breach 2022, IBM Blog https://www.ibm.com/reports/data-breach.
[28]National Cyber Security Policy (draft v1, (Aug. 6, 2013), https://www.meity.gov.in/writereaddata/files/downloads/Nationalcyber_security_policy-2013%281%29.pdf.

that it had developed a draft cyber security plan to secure the country's cyberspace. But there was no discussion on the specifics of the strategy or the execution program.[29]

(B) Information Technology Act, 2000

The Information Technology Act of 2000 was India's first, historical cyber security law. To guide cyber security laws in India, set data security guidelines and control cybercrime, the Indian Parliament passed the IT Act of 2000, which is supervise by the Indian Computer Emergency Response Team (CERT-In). Among several other things, it secures the private sector, e-banking, e-governance and e-commerce.Albeit India in absence of a single, extensive cybersecurity law, it encourages cybersecurity norms through the IT Act and various other sector-specific laws. It also bestowed a crucial legal basis for India's digital infrastructure.

For example, to inhibit sensitive information from being hacked, destroyed, leaked or misused, Indian companies and organizations are required to establish "reasonable security practices and procedures" under **Section 43A of the IT Act** it sets out what will happen to specific acts related to computer resources (such as computers, systems and networks) and computer infrastructure that are operated without the person owning or controlling those resources or infrastructure.

This involves a diversity of actions, including devastation, denial of access, downloading without possession, and computer polluters. If these acts are done dishonestly or fraudulently, they are punishable **under Section 66** with imprisonment of up to three years and/or a fine of up to Rs 500,000.Ahead, whoever get access to material containing personal information of another person and unfold it without that person's consent with intent to cause harm or with knowledge that he is likely to suffer wrongful loss or gain If so, the maximum punishment would be a jail term of 3 years and/or a fine of Rs 500,000. as stated in Section 72A of the IT Act.[30]

- **Tempering of Computer-Generated Documents**
    - When computer source code is need to be stored or maintained by any applicable law, it is illegal to intentionally hide, destroy, or amend the code. Punishable with a fine of up to Rs 200,000 and/or up to three years in jail.[31]

[29]Devesh K Pandey, Draft cybersecurity strategy has been formulated: Centre, The Hindu (Dec. 14, 2022), https://www.thehindu.com/news/national/national-security-council-secretariat-formulated-draft-national-cyber-security-strategy-centre/article66262515.ece.
[30]The information technology act, 2000, § 72, No. 21, Acts of Parliament, 2000 (India).
[31]The information technology act, 2000, § 65

- **Dishonestly Retaining Stolen Resources or Equipment**
    - If any person dishonestly possesses or admit any stolen electronic resource or device, when he knows it to be stolen, he can be punished with imprisonment of up to three years and/or a fine of up to Rs 100,000.[32]
- **Identity Theft**
    - The act of fraudulently or dishonestly using someone else's electronic signature, password, or any other unique identifying features is known as identity theft. It carries a maximum prison sentence of 3 years and a fine of Rs. 500,000.[33]
- **Cyber Terrorism**
    - Cyber terrorism can refer to specific acts (such as unauthorized access or refusal of access to computer resources) that are carried out with the motive to threaten the sovereignty, unity, integrity or security of India or to create fear in the population. Cyber terrorism includes unlawful access to any data or information which has been acquired with reasonable suspicion that it will be used to undermine the interests of sovereignty and integrity of India, security of the State, reputation towards other countries, public order, elegance,or morals, contempt of court, defamation or it may be used to threaten to incitement to commit a crime, or the interests of a foreign country, group of people or other entity. So, the definition of cyber terrorism is quite wide and carries a punishment of life imprisonment.[34]

(C) Indian SPDI Rules For Proper Safety Practices, 2011

The international norms are as per the Indian SPDI rules of 2011, IS/ISO/IEC 27001 norms. While Indian businesses can thus use these norms to help meet "reasonable security practices" wants under Indian law, doing so is not needed, albeit strongly encouraged.In addition to limiting manifestation, data transmission, and security measures, rules could bestow people with the ability to update information they believe is fallacious. They are not responsible for the genuineness of passwords, biometric data, medical records and history, or sensitive personal data (SPD) such as sexual orientation; They apply only to corporate entities.[35]

[32]The information technology act, 2000, § 66b
[33]The information technology act, 2000, § 66c
[34]The information technology act, 2000, § 66f
[35]Information technology (reasonable security practices and procedures and sensitive personal data or information) rules, 3 (Department of Information Technology 2011).

(D) Indian Penal Code

While the IT Act lists specific offences, there are other laws under the general criminal law of India that permit remedies. Cybercrime can be considered a crime under varioussection of the IPC, including:

- **Cheating**
    - Tricking anyone into giving something that they would not have else given falls within the definition of fraud. An example of a cybercrime is tricking anyone into sending secret or restricted information to someone who should not have it – information that the person being deceived would know better than to give.[36]
- **Forgery of Electronic Records**
    - This section bestows specific reference to an act in relation to any electronic document making it a felony. Manipulation of a document or electronic record, which could cause harm to someone else or even fraudulently claim property, is an example of this. If such an act is done with malicious intent, it will amount to forgery and can be punished with a maximum of two years imprison.[37]
- **Receiving Stolen Property**
    - In line with the IT Act offence, a person faces up to three years in jail if he knowingly accepts or possesses stolen property such as an electronic device.[38]
    - **Sharat Babu Digumarti v. Govt of Nctof Delhi,**[39]Nevertheless, it is a well-established tenet that a specific law – in this example, the IT Act – supersedes a general law (i.e., the IPC). So, the charges for conduct of an offense can be filed under IT only if it falls under both IPC and IT Act.

(E) IT Rule 2021

The Ministry of Electronics and Information Technology (MeitY) on February 25, 2021, replaced the IT Rules, 2011 with the Information Technology (Guidelines for Intermediate and Digital Media Ethics Code) Rules, 2021. On June 6, 2022, a little more than a year later, the Indian Ministry of Electronics and IT (MeitY) issued the most recent draft amendments to the IT Act, focused at making it more effective in view of the ever-evolving digital environment.The moved amendments focus to bestow more due diligence on businesses and

[36]Indian Penal Code, 1860, Section 415
[37]Indian Penal Code, 1860, Section 463
[38]Indian Penal Code, 1860, Section 411
[39]Sharat Babu Digumarti v. Govt of Nctof Delhi, Criminal Appeal No. 1222.

 [ISSN 2581-9453]

give regular users of digital platforms the option to seek responsibility and compensation for their claims when their rights are infringed. The IT Rules, 2021 also inflict a much higher accountability of personal data protection on larger social media intermediaries and difference between smaller and more major social media intermediaries based on user numbers.[40]

(F) National Cyber Security Strategy 2020

The Government of India's long-awaited follow-up plan to increase cyber security efforts was the National Cyber Security Strategy 2020. Presently the plan is currently under construction and waiting forassessment by the National Security Council Secretariat as an authoritative guide for stakeholders, policy makers and corporate leaders to inhibit cyber incidents, cyber terrorism and cyber spying in cyberspace. The strategy seeks to increase the caliber of cybersecurity audits, to enable enterprises to conduct a more properevaluation of their cybersecurity architecture and expertise. Once the policy is executed, it is expected that cyber auditors will raise their security norms, which will finally motivate businesses to strengthen their security initiatives.[41]

(G)Digital Personal Data Protection Act of 2023

The eagerly awaited Digital Personal Data Protection Act (DPDP) was ultimately passed by the Indian Central Government on August 11, 2023. The EU's General Data Protection Regulation (GDPR) bestows a wide definition of personal data, which the Act focus to protect. Confining the actions of the data principal and data fiduciary.

Data Fiduciaries under the DPDP are need to:

- Only nominate or work with third-party data processors that have formal contracts need them to follow DPDP methods.
- Before using personal data to make decisions that influence the data tenet or confound in the transfer of personal data, secure that the data is accurate and complete.
- Execute the important organizational structures and technical security steps to guarantee continued adherence.
- Take suitable security steps and audits to secure personal data and prevent breaches.

The Data Protection Board of India was also instituted by the DPDP, which also defined a new

[40]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, (Feb. 25, 2021), https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

[41]Aditya Bhatia, (Aug. 15, 2020), https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf.

class of data fiduciary. Organizations grouped by the government as high-risk censorial data fiduciaries are recognized through risk evaluation. Additional restrictions apply to organizations that are found to be censorial data fiduciaries.[42]

V. FUTURE TRENDS IN CYBERSECURITY

Evolving technologies and trends in the field, such as quantum computing and AI-driven threats.

Cyber security is a field that is constantly changing to accommodate new and evolving trends and technologies. AI-driven risk and quantum computing are two vital areas of focus:

- **Quantum Computing:**

New technology: The possibility for quantum computing to change security and cryptography is spacious, as it represents a huge jump in processing effeciency. Quantum computers use qubits – which are able to represent various states with this – unlike classical computers, which use bits (0s and 1s). As a result, they are far faster than conventional computers at solving complicated issues such as decrypting data.

- **Impact On Cyber Security**

The use of classical public-key encryption method such as RSA and ECC is at risk due to the potential of easy cracking by quantum algorithms such as Shor's algorithms. This is known as an encryption vulnerability allied with quantum computers.

Post-Quantum Cryptography: To secure against quantum attacks, scientists are growing post-quantum cryptography algorithms. These methods are meant to guarantee data security in the post-quantum computing era.

- **Ai-Driven Threats:**

Artificial intelligence can be a helpful tool for cybersecurity, but it can also be used by hackers to repair their attacks. In cybersecurity, the use of AI to generate threats is becoming common.

- **Impacts on Cyber Security**

Malware with artificial intelligence capabilities is more agile and adaptable due to their advanced cognitive capabilities. Malware powered by artificial intelligence is difficult to track because it can change and mimic user behavior. By automating and adopting these tactics, artificial intelligence (AI) can increase the effectiveness of phishing attempts. This can result in phishing emails being so convincing that consumers will have difficulty telling them apart

[42]The digital personal data protection act, 22 D.P.D.P.A. (MINISTRY OF LAW AND JUSTICE 2023).

from genuine correspondence. These new developments in technology and trends are changing the landscape of cybersecurity. To stay ahead of emerging threats, organizations need to take a proactive approach, employ quantum-safe encryption, invest in AI-powered security solutions, and develop a cybersecurity culture that recognizes the potential risks associated with these technologies. And knows how to reduce them.[43]

(A) Recommendation

With the increasing cyberattacks we need to strengthen cybersecurity at every level. The first and foremost important thing with regards to cybersecurity is the level of awareness and training to the internet users. Awareness level and users training are considered as of great importance in cybersecurity within digital space. Security tools like firewall, antivirus software, Intrusion detection systems(IDS), Intrusion prevention systems(IPS) should be updated and kept in their best ways as these are the essential components of cybersecurity and plays a vital role in protecting an individual, an organization or a government's system, networks and data from various threats and help them to combat and protect them from these fast-growing threats. An Individual, group of people, any private organization as well as government bodies to take up some proactive approach,AI driven security solutions, promote cybersecurity culture and implement quantum safe cryptography linked with these technologies.

VI. CONCLUSION

It is the era of cyberspace climate where every individual, group of people and the government itself is using internet worldwide. This excessive dependency on the internet has led a biggest concern that is to strengthen the cybersecurity as excessive dependency on internet has pave ways to cyber attackers to commit cybercrimes easily and leading to the increment of cyber victims at its highest rate day by day. Therefore, cybersecurity is very important for protecting and safeguarding digital space and its ambit and preclude cyberattacks and cyberthreats. It plays a significant role in safeguarding integrity of digital ecosystem, national security and individual privacy in this interlinked and interconnected world. As the cyberattacks are increasing every day and also developing themselves highly advancing tactics and attack vectors therefore it has become utmost important to maintain highly effective cybersecurity and organization's need to be very vigilant, approachable and proactive in diagnosing and tackling these advancing threats in the digital space. It is not going to be one time effort but

[43]Dr. Vishal Waghmare & Rajashree Y Patil, Cyber Security Need of Digital Era: A Review, 182 International Journal of Computer Applications (2018).

will be continuous effort and commitment to protect and safeguard sensitive data and digital assets from these cyberattacks and cyberthreats.

*****

 [ISSN 2581-9453]