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: 7.301
Volume 3, Issue 1, July 2023

A Study on Cyber Security Challenges and Its New Trends in Modern Technologies

Robin Jassal
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *Due to the present way of living, more individuals are accepting technology nowadays and using it for both online shopping and banking activities. While this is happening, securing data becomes more difficult. Online crime, sometimes known as cybercrime, has grown in popularity along with social media's widespread use. Data security is important in the field of information technology. One of the biggest problems in the world today is information security. When we consider cyber security, we first consider "cybercrimes," which are growing significantly every day. In order to prevent this type of cybercrime, several governments and businesses adopt various measures. Plenty of measures have been taken to protect against it, but many people are also extremely concerned. With the rapid advancements in technology, numerous emerging technologies have transformed industries and societies. However, alongside these developments, new cyber security challenges have arisen. This research paper explores the evolving landscape of cyber security in the context of recent technologies.*

Keywords: Cyber security, Cybercrime, Challenges, Artificial Intelligence, Blockchain, IoT.

I. INTRODUCTION

In today's technological environment, many new technologies are changing the lifestyle. But because of these new technologies, we are unable to protect our personal information in a very effective manner, and as a result, cybercrime is on the rise. Nowadays more business transactions are conducted online, therefore this industry needs a high level of security for the most reliable and transparent transactions. Thus, cyber security has emerged as a current issue. The reasons for this massive increase in cybercrime include the usage of inadequate software, outdated security technologies, design flaws, programming errors, easily accessible internet hacking tools, a lack of public awareness, high rates of financial return, etc. The attackers create enhanced attack tools to investigate the target's weaknesses and then attack the victim. As a result, its challenging-to-detect threats in various new technologies. Even the most advanced technologies, such as net banking, and e-commerce, require a high level of security. Since these technologies include some crucial information about a person, their security has turned into a top priority. Each country's security and financial stability depend on improving cyber security and protecting vital information infrastructure. The growth of new services and governmental policy now depend on making the Internet safer and protecting Internet users.A comprehensive and safer strategy is required for tackling cybercrime. It is crucial to provide law enforcement officials with the tools they need to properly pursue and investigate cybercrime because technological solutions cannot, by themselves, prevent every crime. There are now strict laws governing cyber security in many nations and governments, preventing the loss of any important data. To defend themselves from the increased number of cybercrimes, everyone must acquire training in cyber security.

1.1 Objective

The objective of this research paper is to discuss the challenges faced by organizations in ensuring cyber security and the new trends in modern technologies that can help in mitigating these challenges. To understand the evolving nature of cyber risks and their potential effects on both enterprises and individuals. To research the most effective cyber security measures for reducing cyber security threats and safeguarding.

Overall, the research paper aims to provide insights into the current state of cyber security and the new trends that organizations can adopt to enhance their security posture and protect their assets.

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: 7.301
Volume 3, Issue 1, July 2023

II. LITERATURE REVIEW

This section provides an overview of fundamental concepts about the cybersecurity and related terms related to this research

2.1 Cybercrime:

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate the carrying out any illegal act".A cybercrime is a type of crime that targets or makes use of a computer, a connected network of computers, or both for malicious purposes.Investigators often use a variety of techniques to look into gadgets that may be used in or be the target of a cybercrime. A cybercriminal is a person who commits crimes online using their skills in technology. They might be single people or groups. However, when hacking is done with the intention of carrying out any damaging acts, it is regarded a cybercrime, and we refer to this person as a "black hat hacker" or a cybercriminal.

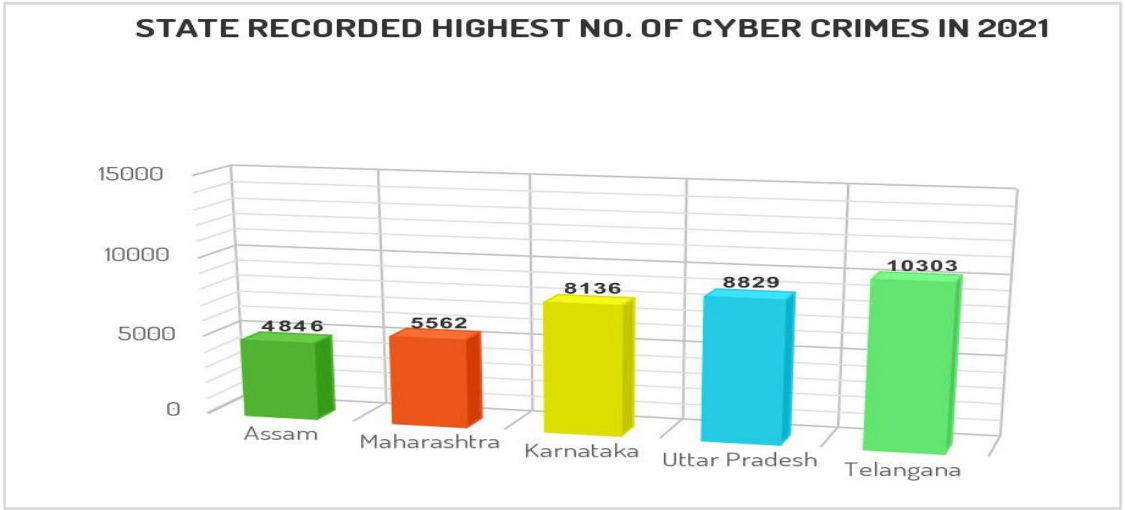
Why are Cybercrimes Increasing?

The world is today heavily dependent on technology since new technologies are continually being developed. The majority of smart gadgets have internet access. Both advantages and disadvantages exist.One of the risks is the big rise in the number of cybercrimes committed.In addition to the fact that hiding your traces is much easier when conducting a cybercrime than it is when committing a genuine crime, various countries may have varied rules and regulations regarding cybercrimes. Below, we cover many factors that have contributed to the significant rise in cybercrimes:

- **Vulnerable devices**: As we previously indicated, a variety of vulnerable gadgets are introduced due to the absence of effective security measures and solutions, making them an easy target for hackers.
- **Personal motivation:** Some cybercriminals use their crimes as a form of revenge against people they despise or otherwise disagree with.
- **Financial motivation**: Cybercriminals and hacker organisations most frequently carry out attacks with the intention of making money.

2.2 Cybercrimes in India

In 2021, India recorded 52,974 cybercrimes, a rise of over 6% from the previous year. According to data from the National Crime Records Bureau (NCRB), Telangana topped the list of states, accounting for more than 19%. In 2021, the state recorded 10,303 instances, a 105 percent rise over the previous year. However, the number fell by 20% and 24%, respectively, in the next two states on the list, Uttar Pradesh and Karnataka.8,829 instances were reported in Uttar Pradesh in 2021, down from 11,097 in 2020. Karnataka saw a decrease in instances from 10,741 in 2020 to 8,136 in 2021.



Source: National Crime Records Bureau (NCRB)

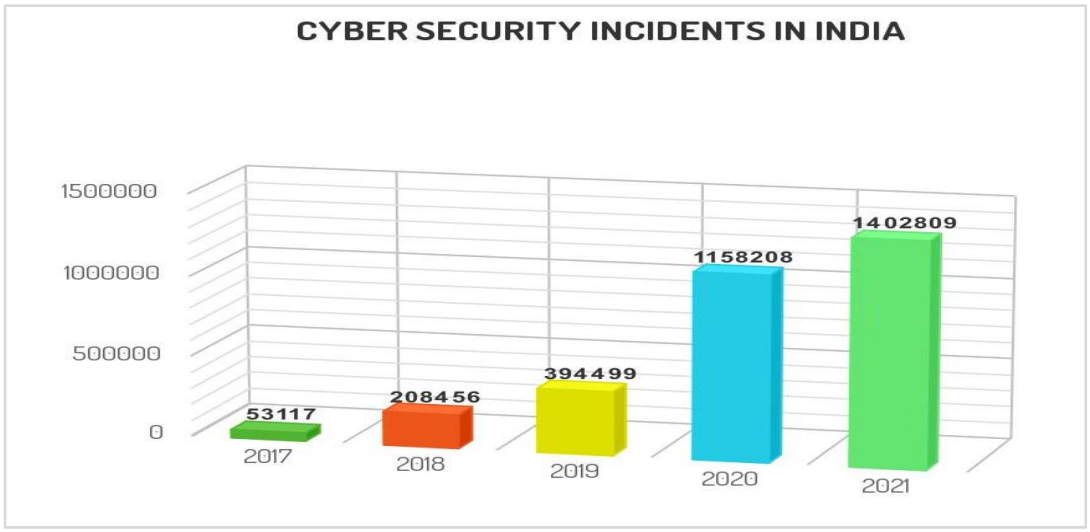
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

2.3 Cyber Security

Today's world is more dependent on technology than ever before, as you can see by looking around. This trend offers several advantages, from nearly instant Internet information access to the latest conveniences offered by smart home automation and concepts like the Internet of Things. It may be hard to accept that potential risks hide behind every gadget and platform since technology has brought us so much good. Despite how positively people view current improvements, cyber security concerns raised by modern technologies create a serious risk. The vulnerabilities in the gadgets and online resources we've grown to rely on are brought to light by the constant growth in cybercrime. This issue leads us to consider what cyber security is, why it's important, and what we should learn. Cybersecurity is a discipline that deals with methods to protect systems and services from malicious online activities including spammers, hackers, and cybercriminals. While certain cyber security components are built to start a strike immediately, most modern professionals are more concerned with figuring out how to safeguard all assets, from computers and mobile phones to networks and databases, against attacks.

Cyber Security incidents in India:

Data indicates that 2022 has been India's worst year ever for cyberattacks, an issue that has only become worse with growing digitalization. According to a survey published by Indusface, a software-as-a-service (SaaS) security firm funded by Tata Capital, India is now one of the nations that is frequently targeted and penetrated. Nearly 59% of the 829 million cyberattacks that the company discovered and stopped globally in the fourth quarter of 2022 were targeted at India. Ransomware attacks have become increasingly frequent in India, and one of the most used attacks in 2022. Government data, collected by the Indian Computer Emergency Response Team (CERT-In) of the Ministry of Electronics and Information Technology, is only available till 2021, but it too indicates an increase in cyberattacks in India. A total of 3,94,499 incidents were addressed by CERT-In in 2019. In 2020, CERT-In analysed 11,58,208 incidents, more than triple the number from the year before. This rise continued in 2021, when 14,02,809 incidents, a 21% increase occurred. Website infiltration, malware propagation, malicious code, phishing, distributed denial-of-service (DDoS) attacks, website defacements, unauthorised network scanning or probing, ransomware attacks, data breaches, and susceptible services are among the issues that CERT-In investigates.



Source: CERT-In

So, it is difficult to minimise the significance of cyber security in the digital age. In today's linked world, a single security breach can have major consequences. These breaches cost the organisations concerned a lot of money and damaged their reputations with customers. Therefore, cyber security is crucial to protecting organisations and people from the potentially disastrous effects of a security breach.

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: 7.301
Volume 3, Issue 1, July 2023

III. RESEARCH METHODOLOGY

The paper adopts a descriptive research design to analyse and understand the cyber security current developments in technology and cyber security challenges. A thorough review of relevant literature is conducted to establish the existing knowledge and understanding of this topic This provides an outline for the study and identifies areas of existing research that need more research. To learn more about emerging trends and difficulties in cyber security, primary and secondary data are gathered. While secondary data is gathered through existing research, reports, and articles. Primary data is gathered through surveys and direct observation. Charts and narratives are used to illustrate the analysed data in order to give a thorough overview. In order to provide a thorough analysis, the research technique of the paper includes both qualitative and quantitative methodologies

IV. EMERGING CYBERSECURITY CHALLENGES

Global cyberattacks rose 38% in 2022 over 2021, according to Check Point Research. The growth of remote work, rising cloud computing usage, and increased cybercriminal proficiency were some of the reasons that contributed to this surge. Data breaches dominated the news in 2022. Data breaches occurred at companies like Twitter, Microsoft, and American Airlines as fraudsters continued to create disruption in businesses, preventing commercial growth and disrupting company stability. The Identity Theft Resource Centre (ITRC) estimates that 422.1 million people were affected by data breaches like this in 2018, an increase of 41.5% from 2021.Here mentioned below the top cybersecurity challenges of the present.

4.1 Ransomware Attacks:

One of the main cyber security issues that concerns everyone in the digital age is ransomware. A record number of attacks with ransomware occurred in 2021–2022, and this trend is expected to continue in 2023.As the word ransom means, it involves getting the user's personal data and stopping them from using it until the hackers receive payment in the form of a ransom. Businesses that require access to their data to carry out their everyday operations now suffer greatly because of this breach, reinforcing the necessity for them to place a major focus on their data security plans. Without paying the ransom, the organisation might be able to get back the data that was taken hostage, but it wouldn't guarantee that the bad guys wouldn't try to get their hands on the data.

Because of this, users should focus on frequently backing up their devices, using the latest anti-malware and anti-phishing tools, and keeping them constantly updated. In addition, as every piece of information was distributed digitally following the pandemic, an increasing number of these attacks were recorded.

4.2 Phishing Attacks

Phishing is a form of social engineering that targets consumers' login credentials and payment card information. Here, the information is to the hacker's advantage as compared to ransomware. A popular service provided by Google for both personal and business use is Gmail. Now, anytime you access your mail account, you can see a spam folder containing emails that the platform has identified as a risk to the security of your data. Your mailing partner has identified hundreds of phishing attacks in these spam emails and has alerted you to the possible cyber threat they pose. However, some of the correspondence still makes it to your inbox, where you can accidentally fall into a trap.Using anti-phishing technologies like antivirus software and an anti-phishing toolbar, sandboxing email attachments, and informing staff are a few techniques to prevent phishing attempts.

4.3 Cloud cyber-attacks:

Big businesses like Amazon, Google, and Microsoft all provide cloud computing platforms, which has helped the technology's popularity soar in recent years. The technology, which was initially developed as a backup storage solution, is today an all-encompassing computing platform that has significantly changed how businesses use, save, and exchange information. However, as cybersecurity experts are aware, everything that gains popularity in the digital age is going to attract the attention of cyber criminals. Cloud computing platforms are no exception. Attacks on these sites have rapidly increased in recent years. The third most targeted cyber environment in 2021, cloud computing platforms accounted for 30% of all cyberattacks. The present era of new technology known as cloud computing changed the

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: 7.301
Volume 3, Issue 1, July 2023

actual world of data storage. Cloud services are widely used by businesses of every kind to store user-sensitive data. Although its use has reduced costs and increased productivity, it has also increased the possibility of data security breaches. The absence of encryption, lack of authentication, and inappropriate use of cloud services are the major causes of compromised data security. To preserve the integrity of the sensitive information, they must maintain several concerns for cloud security and data protection. By being aware of the principles of cloud security and some of its most common weaknesses, we may lessen our chances of becoming victims of cyberattacks.

4.4 Software Vulnerabilities

Another major challenge faced by cyber security is software vulnerabilities. A software vulnerability is a weakness in the software code that can be used by cybercriminals to break into secure networks and steal confidential data. Software vulnerabilities present a challenge since they can be hard to detect and can stay undetected in software for years.Software vulnerabilities continue to be a problem in cyber security for a number of reasons. One factor for this is the growing complexity of software, which makes it more challenging to find flaws.Thesoftware is often developed quickly and under tight deadlines, which can lead to lapses and errors in the code.Also, because software is frequently used for many years after development, vulnerabilities may exist for a long period before they are found.

4.5 Inside Threats:

Insider threat is a growing challenge in cyber security. A security risk that emerges within an organisation is known as an insider threat. Employees, contract workers, or other people with access to private data or systems may be responsible for this. Insider risks can seriously harm an organization's security and reputation, whether they are intentional or accidental.Insider attacks remain a challenge in cyber security for a number of reasons. One reason is that it is hard to identify fraudulent activity when insiders have authorised access to an organization's systems and data.Insiders may also be more familiar with a company's security protocols and weak points, which might make it easier for them to go past security protocols.Insider threats can take many different forms, such as stealing secrets, destroying systems, and gaining unauthorised access to confidential data. The methods that insiders employ to carry out their attacks can include social engineering, phishing, and malware.

V. COUNTER MEASURES

Employee Training and Awareness: Using employees as an entry point is one of the most popular methods that cybercriminals access your data. Training your staff on cyber-attack prevention and informing them on current digital threats is one of the most effective strategies to guard against cyber-attacks and all forms of data breaches. They should check links before you click them. Check the email addresses in the received email.

Regular Software Updates: Your operating system may be a vulnerable target for attackers since it manages every aspect of your device. Operating systems provide a number of security features that help avoid attacks. However, the problem is that cyber-related risks are always changing. Because of this, operating system providers frequently release updates: must keep up with the constantly evolving risks that cybercriminals offer. So, it's important to keep all operating systems, firmware, and software applications updated with the most recent security patches. Regular updates assist in addressing identified vulnerabilities and safeguarding against possible exploitation.

Setting Up Next-Generation Firewalls: Next-Generation Firewalls (NGFWs) are advanced security systems that include more security features and capabilities than conventional firewalls. They provide today's networks more visibility, management, and security. NGFWs provide SSL/TLS inspection, advanced threat intelligence, deep packet inspection, intrusion prevention systems and application awareness. They provide for enhanced control over network traffic by enabling organisations to set precise security policies based on apps, users, and content. Additionally, NGFWs interface with current security systems and offer continuous surveillance, threat information feeds, and proactive threat detection and response. The deployment of NGFWs is a critical step in enhancing network security inside an organisation and managing the changing threat environment.

Multi-factor authentication (MFA): This is a security measure that adds an extra layer of protection to user accounts and systems by requiring multiple forms of verification before granting access.MFA ensures stronger authentication by combining everything the user knows (like a password), something they have (like a physical token or mobile device),

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: 7.301
Volume 3, Issue 1, July 2023

and something they are (like a fingerprint or face recognition). Organisations may considerably improve their security posture and lower the risk of unauthorised access and data breaches by using MFA. Even if a user's password got into the hands of an attacker, they would still require the extra factor(s) to get access. Attackers will find it considerably harder to breach accounts and systems as a result.

Backup and Recovery: Backup and recovery are essential components of data management and cybersecurity. It involves creating copies of critical data and systems in order to protect against unintentional loss, data corruption, hardware failures, natural disasters, cyberattacks, and other occurrences that might result in data loss or system outage. In contrast, recovery refers to the act of restoring backed-up data and systems to their initial state following a data loss incident or system failure. This may include recovering data from backups, rebuilding systems, and guaranteeing the data's integrity and availability. To maintain the availability, integrity, and security of their data, organisations of all kinds must have an adequate backup and recovery strategy.

VI. NEW TRENDS IN MODERN TECHNOLOGIES

Artificial Intelligence technology: AI is emerging as major trend in cyber security. By automating tasks that would normally take a long time or be impossible for people to do, these technologies are used to improve cyber security measures. Cybersecurity applications of AI technology include the following:

AI-based User Behavior Modeling: Some cybersecurity attacks that target business networks involve the theft of data from certain users within the organisation. It can be difficult to find and prevent malicious users who pretend to be as users in order to access the business network using technically legitimate means. Cybersecurity solutions powered by AI can identify the usage behaviours of certain users and track changes to those usage patterns. To put it another way, technology alerts the security team when something occurs. Darktrace has placed into effect a cybersecurity solution that makes use of machine learning to examine raw data from network traffic in order to figure out the original state of every user’s and device’s usual behaviour within an organisation. When a major deviation from normal behaviour is detected, the system uses training datasets and expert-provided raw data to identify it and instantly alert the organisation of the threat.

Malware Detection: Cybersecurity is significantly affected by malware. Machine learning algorithms are used by AI-based solutions to identify and address known and undiscovered malware threats. Large data sets may be analysed by machine learning algorithms to find patterns and anomalies that are challenging for people to identify. AI can find new and undiscovered malware types that conventional antivirus software might overlook by examining the behaviour of the a virus. It is possible to train AI-based malware detection tools using both labelled and unlabeled data. Data that has been labelled with certain features, such as whether a file is dangerous, is referred to as labelled data. The machine learning algorithms may be trained to find patterns and anomalies in unlabeled data, which is not labelled.

Blockchain Technology: Blockchain is a decentralised, open-source digital ledger technology that securely records and verifies transactions among multiple devices or computers. Through the use of decentralised procedures and cryptographic hashes, it guarantees the accuracy and transparency of data. Beyond cryptocurrencies, blockchain technology has other uses as well, including secure data storage, supply chain management, digital identity verification, and more.Due to its unique features that potentially improve data security, authentication, and privacy, blockchain technology has attracted interest in the field of cybersecurity. The use of blockchain technology in cybersecurity is on rising in the following ways:

Immutable and Tamper-Resistant Data: Because blockchain technology is decentralised and distributed, data kept there cannot be changed or tampered with without the network's participants' permission. Blockchain is beneficial for safeguarding sensitive data due to these characteristics, including digital identities, financial transactions, and supply chain data.

Smart Contracts for Secure Transactions: Smart contracts are self-executing contracts that automatically carry out predetermined activities when specific criteria are satisfied. Smart contracts can enable safe and tamper-proof transactions without the need for middlemen, lowering the danger of fraud or manipulation, by using the security and immutability of the blockchain.

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: 7.301
Volume 3, Issue 1, July 2023

Decentralised threat intelligence: Blockchain can make it easier for organisations to share threat intelligence while maintaining trust and confidentiality. Blockchain-based decentralised threat intelligence platforms enable the safe and anonymous exchange of threat information, strengthening organisation protections against online attacks.

Behavioral Biometrics Authentication:
A technology known as behavioural biometric authentication verifies a user's identity by using their behaviour. It accomplishes this by continuously monitoring their physiological and/or behavioural characteristics and comparing the patterns to data about the user that is recorded on the device.Behavioral biometric authentication is different from traditional authentication techniques.It continuously verifies user identities and evaluates how they interact with their devices in real time. This increases security since it separates legitimate users from online criminals by identifying people based on their interactions and online behaviour

Internet of things:
The Internet of Things (IoT) is a network of physical devices, including gadgets, cars, appliances, and other objects, that have sensors, software, and network connectivity built into them to enable data collection and sharing.IoT device proliferation creates new security issues. To avoid unauthorised access, data breaches, and possible disruptions caused by compromised IoT devices, it is essential to ensure the security of networks and linked devices.The most widely used IoT security technologies are listed below:

IoT Network Security:
IoT network security is more difficult than traditional network security due to the wider choice of communication protocols, standards, and device capabilities, all of which present serious problems and added complexity. It involves protecting the network connectivity that connects IoT devices to the back-end internet infrastructure. The capabilities include firewalls, intrusion prevention and detection systems, and typical endpoint security features like antivirus and antimalware. Vendors like Cisco, Darktrace are examples.

IoT Encryption:
Ensuring data integrity, preventing data sniffing by hackers, and encrypting data in transit and at rest between IoT edge devices and back-end systems. Standard encryption procedures and protocols are restricted by a number of IoT hardware profiles and devices. Additionally, since inadequate key management would lower overall security, every IoT encryption must be included with corresponding complete encryption key lifecycle management mechanisms. Cisco and HPE are two examples of vendors.

IoT Security Analytics:
Using this technology, data from IoT devices is gathered, aggregated, monitored, and normalised while also delivering proactive reporting and alerting on suspicious activity or activity that deviates from set policies.Although these capabilities are still developing, these solutions include advanced machine learning, artificial intelligence, and big data approaches to increase predictive modelling and anomaly detection. To identify IoT-specific threats and intrusions that are not detected by conventional network security solutions like Firewalls, IoT security analytics would be increasingly necessary. Cisco, Kaspersky Lab and SAP are a few examples of vendors.

VII. CONCLUSION

With each passing year, cybercrime continues to take on new forms, and with it, the security of information. To protect the safety and security of sensitive data, enhanced cybersecurity measures have become necessary due to a surge in cyberthreats and attacks. Artificial intelligence, IOT and blockchain technologies are some of the current trends in cybersecurity that present fresh opportunities for improving cybersecurity. But they also bring with them new challenges that are looking for answers. As a result, in order to protect themselves from possible threats, stakeholders must continue to be cautious and proactive in understanding and mitigating cybersecurity risks. It is essential that all stakeholders in the cybersecurity ecosystem work together. We can only effectively tackle cyberthreats and ensure a

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: 7.301
Volume 3, Issue 1, July 2023

safe and secure cyberspace through collaboration and information exchange. Finally, to keep up with the evolving landscape of cyber threats, there is a need for ongoing research and development in the field of cybersecurity. While there is no ideal solution to cybercrime, we should try to reduce it using some of the following the above-mentioned measures can help to reduce cybercrimes.

REFERENCES

[1]. Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole
[2]. Computer Security Practices in Non Profit Organizations – A Net Action Report by Audrie Krause.
[3].A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments Yuchong Li, Qinghui Liu.
[4]. Issues regarding cybersecurity in modern world by H. Geldiyev, M. Churiyev, and R. Mahmudov