EXPLORING CYBER SECURITY CHALLENGES AND EMERGING TRENDS IN LATEST TECHNOLOGIES

Dr.Supriya Nagarkar, Ms. Suvarna Ghonge, Faculty, Dept. of Computer Science Tilak Maharashtra Vidyapeeth, Pune-37

Abstract
The rate of online criminal activity, sometimes referred to as cybercrime, has increased as more individuals use social media. More and more people are accepting technology nowadays and using it in their online shopping and banking activities, given the kind of lives they currently lead. At the same time, preserving information has become increasingly difficult. To advance technology, data security is crucial. Right now, one of the biggest issues is information security. We quickly think of the rising number of cybercrimes every day when we think of cyber security. To combat this type of cybercrime, several governments and companies implement a range of security measures. The public is quite anxious despite the fact that there are several internet safety initiatives. In this essay, the danger that developing technologies pose to cyber security is the main point of concern. Additionally, it underlines evolving cyber security technologies, advancements that have an impact on those technologies, ethical concerns, and inventions that have an impact on cyber security. According to recent research by a number of academics and experts, wireless communications systems and technologies are susceptible to a variety of attacks. These attacks hurt commercial businesses as well as governmental organisations. Hackers are always looking for new ways to circumvent security precautions and are using strong tools and techniques to crack any number of keys, endangering the confidentiality of sensitive and private data. This essay not only talks about the difficulties that the field of cyber safety must face, but it also thoroughly examines the many cutting-edge online safety standards that are already in use.
Keywords: *Cyber security, latest technology, social media trends, Information technology*.

Introduction

Cyber security is one area in which it becomes essential in information technology. Security of information is one of the main concerns of today. The initial thing that springs to mind when we think of cyber security is "cybercrimes," that are at present continuously on increasing frequency. Many governments and companies are implementing a variety of safety measures in an effort to stop these cybercrimes. Many people continue to have grave concerns about cyber security in spite of these safety precautions.The main focus of this essay is on the difficulties of adopting cutting-edge technologies for cyber security. It also highlights the most recent advancements in computer security practises, a code of action, and living that are influencing the industry as a whole [1].

As a result of the digitalization process, which has impacted every aspect of human existence, including healthcare, education, business, and others, sensitive data has been preserved throughout time. The quantity and complexity of cybercrimes increase along with the rapid advancement of technology. Security is the act of protecting digital information from harm on a physical or financial level while maintaining its confidentiality and usability. Many variables, such as the use of insufficient software, out-of-date safety precautions, shortcomings in design, coding mistakes, readily available internet hacking tools, a lack of public knowledge, a high level of financial return, etc., have been blamed for the precipitous increase in cybercrime. Technology-based hackers develop stronger attack tools that they use to first identify the target's shortcomings before attacking the individual in question. As a result, multiple new, challenging-to-detect threats emerge. The increased reliance on the internet in many areas of daily life, the massive amounts of digital data generated by transactions over the internet, and the decentralized nature of storage facilities for data have all contributed to the creation of effective security solutions. Since cybersecurity continually evolves, it is difficult to keep up with newly discovered problems. Because sophisticated hacking efforts are so common, protecting cyberspace is the most difficult and difficult accountability.

Therefore, it is necessary to examine the ideas underlying safety defences, different approaches, and today's difficulties in the field of security for information [2].
The internet's worldwide reach has expanded dramatically in the past few years. Because of the uncommon increase of knowledge that is accessible to them, individuals with unfavourable intentions have more chances. Safeguarding of devices and networks against unusual behaviour is essential. Cybersecurity refers to the preservation of the honesty, freedom of action, and transparency of computer assets that belong to one organisation or are connected to the internet belonging to another. Due to the rapid growth and development of online dangers, many academics believed it was crucial to impart the key concepts of cyber-security to the next generation. Internet crimes are influenced by consumer responsibility in terms of cyber safety while knowledge. In reality, the computer network guide promotes the early detection of weaknesses and the rapid sharing of information about potential threats that may occur in the defence of a number of corporations, including the environment, business, and structures [3].Due to the high expenses required, many businesses typically ignore this cybersecurity threat control, but they also lose out on potential long-term advantages. Although it is apparent that investing in modern technology significantly boosts security, smaller, more recent enterprises have a difficult time accepting this. In many ways, technology improves our daily lives. Contrary to the status quo of traditional business methods, it has achieved progress. Corporate strategy, as well as the total cost and value of goods and services, are all impacted by new technologies. The act of trading one item for another may be used to define business in a straightforward manner. It relates especially to the exchange of goods and services for cash when selling or purchasing those[4].

Over the last two decades, the Internet has been crucial to worldwide communication and has ingrained itself more and more deeply into peoples' life. Internet, today has almost a billion users globally, greatly enhancing its use and performance. Since the World Wide Web has established such a vast global network, the worldwide marketplace now earns billions of dollars yearly. The bulk of contemporary international relationships and operations in the fields of commerce, social media, culture, and government take place online. Conversations between people with disabilities, non-governmental groups, and governmental organisations are involved in this. A significant amount of sensitive and crucial data is carried to the cyberspace or, preferable, handled, controlled, and used across this domain, where essential infrastructures and systems may also be found [5].
The Internet of Things is an enormous collection of people and connected items who collaborate to gather and exchange data pertaining to human behaviour and the surroundings. The IoT ecosystem's embedded devices, which comprise a combination of CPUs, sensors, and communications circuits, allow smart objects to receive, transmit, and react to data produced by the surroundings. These Internet of Things devices communicate with an entry point or another edge device to share sensor data with one another. Both a local processing facility and an online platform are used to analyse the data. These electronic gadgets often convey news, and they function in accordance with that transfer. The Internet of Things presents unique challenges in terms of device compatibility, confidentiality of information, and security. One of the biggest difficulties the IoT presents is keeping it secure. These electronic gadgets track personal information, including the communications and activities you engage in at work and at home. IoT dependability is crucial for user trust, but data security has a spotty history. Many linked systems fail to effectively secure user and device data while it is structured and in transit. Although software bugs are regularly discovered in well-known programmes as well, many Devices connected to the Internet of Things cannot be improved, thus rendering them uneasy by nature. IoT devices like router and cameras are commonly target by hackers who use them as part of huge, connected botnets due to their inherent lack of assurance[6].
The significance of cybersecurity research has dramatically expanded as a result of technological innovation. All business sectors now face a much greater number of cybersecurity-related issues. Big businesses are more worried about when a cyberattack will happen than if one will. Businesses are pleading with governments to stop cybersecurity threats because these problems are costing society a lot of money. Sixty-one percent of small and medium-sized firms have reported having been the

victim of cyberattacks, which have a substantial negative impact on organisations. Similar to this, a second study found that dangers related with cybersecurity, such as data theft and the leakage of secret information, are growing as sensitive cloud technologies and internet-based apps are used more often [7].
Hackers will be able to bypass all subsequent defences if they have access to a network's initial line of defence. The defender should be more driven to examine security at all levels utilising tools in order to spot holes before attackers do. The vast majority of respondents assert that they can locate and identify crucial data on an organization's systems, get access to it, and breach it in less than 15 hours. Currently, the bulk of industry studies show that it takes 200 to 300 days on average between a breach and its discovery. It is clear that online criminals continue to outnumber online security guards. It is essential to situate the problem of cybercrime in a multidisciplinary framework, according to Thomas Holt from the School of Criminal Justice at Michigan State University [8].
A variety of new and emerging technologies are progressing significantly concurrently with these changes. These changes may have an important effect on the type, scale, and possible effects of cyber-attacks against NATO. The rate of technology development is predicted to accelerate over the following ten years, and might have an important influence on military and safety issues. Maintaining NATO's ability to offer resilience and suppleness in the cyber the world requires a comprehension of the impacts of these innovations' rapid rate of shift, complexity, and ambiguity. This report explicitly examines cyber risks that might arise from the creation and application of a variety of new and upcoming technologies during the course of the next 10 years. Before proposing potential steps that NATO and its member states might take, it first highlights intersecting implications for a potential cyber threat situation [9].

Even the most sophisticated technologies, including cloud computing, mobile devices, online banking, and e-commerce, need high levels of security. Because such gadgets include some extremely sensitive personal information about a person, their security has emerged as the most crucial concern. The improvement of cyber security and the protection of vital infrastructure are necessary for the security and economic development of every nation. Making the World Wide Web safer is increasingly essential for the expansion of new businesses as well as government initiatives. A complete and safer technique must be used to tackle cybercrime. Given that technological advancements cannot, in and of themselves, prevent all crimes, it is crucial to provide law enforcement agencies with the funding they require to effectively battle and prosecute cybercrime. There are currently strict laws controlling cyber security in many nations and governments with the aim of preventing the manipulation of any important data [10].
Improving the present security framework is an important goal in the ongoing attempt to protect organisations and businesses versus the threat posed by information theft and cybercrime. Technology-based network security methods like intrusion detection, firewalls, and biometric devices provide a somewhat valid line of defence against a variety of threats. All dangers to the organization's security are believed to originate from within the organisation and not from outsiders or opponents, which is the fundamental idea driving these actions. Early cybersecurity supporters contend that human factors within the framework constitute one of the main obstacles in creating good information security regulations. Tests in accessibility demonstrate that the average end user likely finds safety processes and infrastructure to be perhaps too complex or too sophisticated to comprehend and utilise efficiently. More emotionally connected aspects, it was claimed [11].
Developing countries, especially those in Africa, have generally lagged behind developed ones in the development and use of the Internet. According to figures recently issued by the International Telecommunications Union, or ITU, developing nations now make up a sizable share of Internet users, with 2.3 billion users compared to one trillion dollars among industrialised countries. As a result, despite having a low Internet penetration rate, emerging countries are gradually rising to prominence as big Internet users. They gain from every perk that the Internet has to offer. For instance, businesses may now forge international connections with new suppliers or clients, which

lowers the cost of exchange while boosting productivity and speeding up the transactional process. [12].

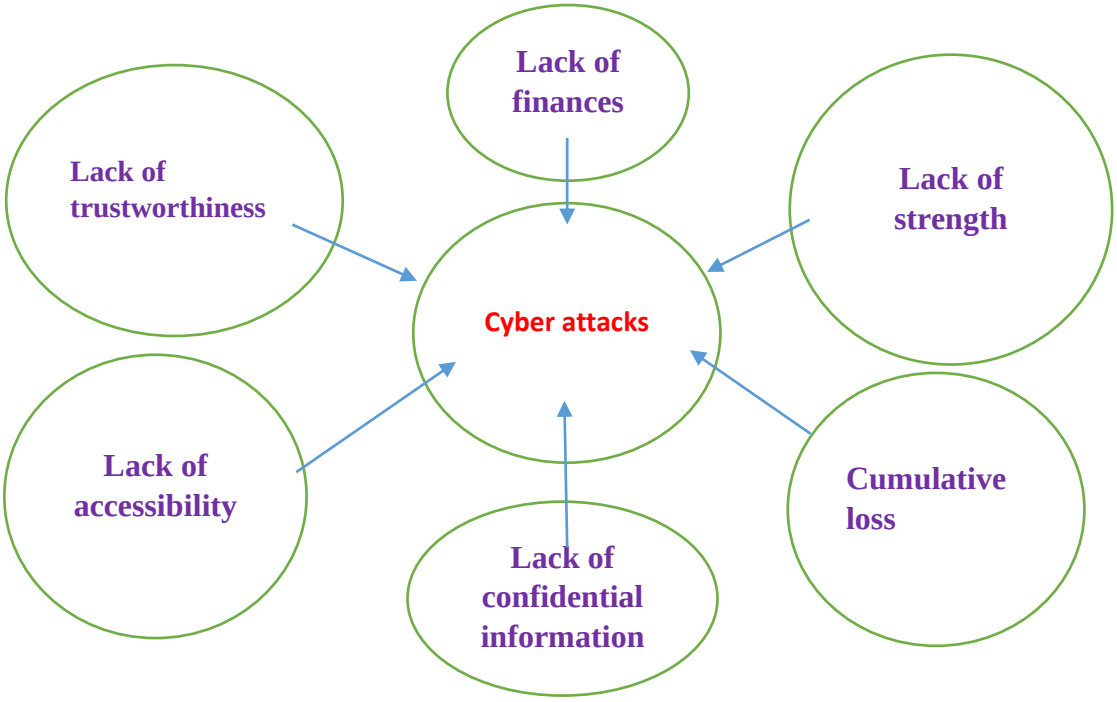

Fig. 1: Framework of cyber attacks

Analysts in bigger businesses and governmental entities, particularly national level cybersecurity centres, are often able to create insight by swiftly identifying, analysing, resolving, and documenting vulnerabilities and assaults over the internet. However, there are challenges with how to construct projections due to the exponential rise in digital threats and vulnerabilities. As a result, security experts are unable to do their anticipated job with the rate at which essential data is released. As a result, vital trends were either overlooked or later found. This may have a bearing upon the creative cyber abilities used by companies that rely on prediction. Rapid changes in the security threat landscape can make it difficult for businesses to maintain business continuity and put their security strategy at danger of change. By automating the human process or providing forecasting analysts with the right decision support tools, uncertainty may be reduced or future events may even be predicted. Major strides have already been achieved in this area by government organisations, academic institutions, and private industry. However, predicting vulnerabilities and threats is a challenging process. A popular method to provide reliable data is to forecast time-series patterns ofcyberattacks using information through different modes [13]. Online safety depends on the precautions people take and the decisions they make when they set up, manage, and use computers and the Internet. Private data and technical resources must be physically protected from unauthorised access using technological means as part of cybersecurity. The issue of end-user mistakes must be tackled by cooperation and partnership between the general business community and the relevant technical industries, as well as with the important support of top management [14].

A diversity of data may now be stored in databases thanks to the development of the internet in all spheres of human life. As technology has advanced, preserving and protecting the security of data is becoming increasingly important because of the sensitive nature in digitally stored information. Lack of data can lead to data loss from hackers or viruses infestations, which can have far more damaging consequences. In recent years, cybersecurity has become a vital tool for maintaining core values like equality, justice, liberty, and user or organisational privacy while preserving trust and confidence in the internet's infrastructure. Information security is generally referred to as "cybersecurity." As events relating to cybercrime continue to rise, communities in academia, industry, and institutions are worried about safeguarding digital assets from cybercriminals, hacktivists, and particularly vigilant attackers [15].

Worldwide, detailed action plans outlining how smart cities, including those still in the development phases, it is still necessary to create the telecommunications and information technologies which would react to any cyberattacks on their buildings and infrastructures. Flaws in any one component can have broad impacts since all structures are inherently interdependent. As a result, ideas must be made available to the bodies in charge of deciding on and approving the technology that will be used in smart urban regions throughout the globe. As they grow and include cutting-edge digital technology, smart cities are more susceptible to cyberattacks. Cybersecurity, the effort to protect data, communication networks, and essential infrastructure against breaches and crimes, is a crucial element of the development of smart cities. Despite the fact that cybersecurity is becoming increasingly crucial, more study is still required to fully understand the societal, economical, and cultural barriers that prevent cybersecurity practises from being adopted in smart cities throughout the world. It will be important to address these problems and give cybersecurity the greatest attention if smart cities are to maintain their safety and sustainability as they gain popularity[16].
Over the course of the past ten years, ICT advancements have been playing an important part in the rapid development of technology. The way people communicate, go about their livelihoods, and travel are all being significantly changed by this.To be able to establish an extensive network of effective urban services, intelligent cities must integrate new ICTs with already-existing systems for support, depending according to the definition. A population centre known as a smart city links its social, commercial ones, and information technology infrastructures to increase the city's whole collective intelligence. The research is straightforward that one of the key objectives of smart cities was to enhance the quality and efficacy of municipal facilities while also enhancing the administration of public resources and eliminating expenditures on operations, despite the lack of general agreement on what really makes a smart city [17].

Targets included systems, data, and individuals with special interests whose access or breach might be advantageous to users or unauthorised parties. The objectives in this section may be broken down into three categories: data systems, human systems, and technology for information and communication. ICT is the moniker given to physical and networked systems which share characteristics in common, such as processing capacity, data processing, and connections to networks, and that allow us to accomplish tasks with pleasure because of their associated architecture. These types of companies are usually the targets of cybercrimes. Local computer networks which are not linked to the World Wide Web or their main communication routes are becoming the target of attacks as well. They are also referred to as protected internet. One of the most worrisome cases is possibly the JPMorgan Chase one. Attacks were carried effectively via auxiliary hardware; hackers used, and even contaminated, POS and ATM hardware to access the bank's computer system and work secretly for a period of time exceeding one month. The use of information technology has grown significantly since the development of the Internet. People and organizationsutilize technology for critical tasks like banking, managing workers, or cooperating. While IT makes those duties easier, it also presents significant safety issues which must be dealt with by everyone, from people to government organisations[18].
Defence and intelligence agencies frequently treat cyberattacks as problems of national security when responding to them. As a result, there have been instances where cyberthreats have been overclassified, where corporations and the government have been embroiled in ongoing battles, and where the negative effects of illicit internet use on society as a whole have gone unacknowledged. The initial half of the essay concentrates on the way cyberattacks impact civilization as a whole, especially the energy, transport, and health sectors, while additionally presenting an argumentative basis for cybersecurity. The remaining portion examines how the internet has been used to exacerbate chasms between communities of identity, to promote incohesion, and to create complications related to societal safeguards. It does this by looking at the history of cyberconflict[19].
Organisations now face a threat to the security of their information due to an increase in data breaches. However, the great majority of organisational security risks are brought on by human

factors since employees routinely disobey organisational rules, which can result in security incidents that are either directly or indirectly caused. Previous studies have suggested that users' internal variables, such as attitude, self-efficacy, and expected reaction cost towards security tasks, may have an impact on their commitment to upholding privacy laws. Security self-esteem is often used to describe a person's safety knowledge and skills that allow them to fulfil their security obligations and adjust to changing security demands. In light of what was said above, people who are ignorant about technology security concerns may feel more insecure, unsatisfied, and helpless, which makes it challenging for them to deal with security difficulties in real-world situations. Staff members usually struggle to work together to find a solution to tackle cyber security issues as a result. The purpose of this study is to examine the types of security information that employees exchange and debate through various workplace communication channels, as well as to assess how such channels affect users' safety behaviours. Understanding user security behaviour sharing strategies can help businesses create and develop channels that will increase staff awareness of cyber security concerns and encourage them to uphold security duties. Researchers also discovered that these techniques usually fall short of effectively disseminating the required knowledge.An organisation can not only motivate employees to learn more by creating a culture where people are always willing to share knowledge and have a reliable channel of communication, but also reduce the risk of external attacks by raising internal awareness of information security and compliance with internal policies[20].

Conclusions

Cyberattacks commonly target personal and business information from individuals and organisations. Technology obviously provides new methods to do business as well as many other benefits, but there will always be safety issues. Although companies consistently make significant investments to address the problem, it remains challenging. E-commerce security has to be improved and invested in if an online firm is to gain a competitive advantage and be profitable. Nobody can afford to pay the cost of losing customers' trust as a result of the release of their personal information. Rigid monitoring measures must have been carried out prior to an occurrence, on both the organisational and consumer ends. Secure passwords and exercising caution while clicking and downloading anything are only two examples. Though it has an appealing title and is essential for the present commercial sector, online shopping faces cyber security issues. The current situation necessitates making investments in safe e-commerce technologies and making preparations in advance. The difficulty of threats to cyber security persists like a sword aimed at causing damage a company that an unanticipated time, regardless of the extent to which consumers and employees have been taught and proficient when performing online shopping, how much the internet retail firm conducts and concentrates on the execution of cyber security protocols and regulations, and the manner in which much new technology is used.

Usability issues are also becoming more and more crucial as a way to intuitively learn about and apply end-user-oriented security measures without making them complicated or necessitating steep learning curves in order to protect the data. The community's cyber safety practises are strengthened through the adoption of creative patches that solve current security and confidentiality challenges.

References

1. Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842*.
2. Rajasekharaiah, K. M., Dule, C. S., &Sudarshan, E. (2020, December). Cyber security challenges and its emerging trends on latest technologies. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 2, p. 022062). IOP Publishing.
3. Kaur, J., &Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.
4. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in psychology*, *13*, 927398.

5. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.
6. Tariq, U., Ahmed, I., Bashir, A. K., &Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117.
7. Mahmood, S., Chadhar, M., &Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*, 1-11.
8. MaalemLahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 1-18.
9. Bellasio, J., &Silfversten, E. (2020). The impact of new and emerging technologies on the cyber threat landscape and their implications for NATO. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, *88*.
10. Rajasekharaiah, K. M., Dule, C. S., &Sudarshan, E. (2020, December). Cyber security challenges and its emerging trends on latest technologies. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 2, p. 022062). IOP Publishing.
11. Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In *Research anthology on artificial intelligence applications in security* (pp. 1960-1977). IGI Global.
12. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28(3), 269–282.*
13. de Boer, M. H., Bakker, B. J., Boertjes, E., Wilmer, M., Raaijmakers, S., & van der Kleij, R. (2019). Text mining in cybersecurity: Exploring threats and opportunities. *Multimodal Technologies and Interaction*, *3*(3), 62.
14. Tonge, A. M., Kasture, S. S., &Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of computer Engineering*, *2*(12), 67-75.
15. Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., &Sakib, N. (2022, May). A review of quantum cybersecurity: threats, risks and opportunities. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-8). IEEE.
16. Alhalafi, N., &Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities*, *6*(3), 1523-1544.
17. Alzahrani, N. M., &Alfouzan, F. A. (2022). Augmented reality (AR) and cyber-security for smart cities—A systematic literature review. *Sensors*, *22*(7), 2792.
18. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005.
19. Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, *5*(3), 449-470.
20. Pham, H. C., Ulhaq, I., Nkhoma, M., Nguyen, M. N., & Brennan, L. (2018, December). Exploring knowledge sharing practices for raising security awareness. In *Proceedings of the Australasian Conference on Information Systems (ACIS), Sydney, Australia* (pp. 3-5).