IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Issues And Challenges In Modern Business Enterprises In Karnataka

[1] Pradeepa Kumar K V, [2] Dr. Ajoy Joseph,

[1]Research Scholar, Srinivas University, Mangalore.

[2]Professor and Head – MBA Department Srinivas Institute of Technology, Mangalore

Abstract: The rapid digital transformation in Karnataka's modern business enterprises has significantly enhanced operational efficiency and market reach. However, this shift has also exposed organizations to escalating cyber security threats, including data breaches, ransom-ware attacks, phishing scams, and insider threats. As businesses in Karnataka increasingly adopt cloud computing, IOT, and AI-driven technologies, the complexity of cyber risks intensifies, necessitating robust security frameworks. This research paper examines the key cyber security challenges faced by enterprises in Karnataka, including inadequate security infrastructure, lack of employee awareness, regulatory compliance gaps, and emerging threats from advanced persistent threats (APTs). The study also explores mitigation strategies such as AI-based threat detection, cyber security training, and adherence to global standards like GDPR (General Data Protection Regulation) and India's DPDP (Digital Personal Data Protection) Act. By analysing real-world case studies and industry trends, this paper provides actionable insights for businesses to strengthen their cyber resilience and safeguard critical assets in an evolving threat landscape.

Keywords: Cyber security, Digital Transformation, Karnataka Enterprises, Data Breaches, AI in Security, Regulatory Compliance, Cyber Resilience.

1.**Introduction**

In the digital age, cyber security has become a critical concern for businesses worldwide, and Karnataka, India’s leading technology and start-ups hub is no exception. With Bengaluru at its core, Karnataka hosts numerous multinational corporations, IT firms, and burgeoning start-ups, making it a prime target for cyber threats. As businesses increasingly rely on digital infrastructure, cloud computing, and IOT enabled systems, they face growing vulnerabilities to cyber-attacks such as data breaches, ransom-ware, phishing, and insider threats.

The rapid digitalization of business operations, coupled with the adoption of emerging technologies like artificial intelligence (AI) and block chain, has expanded the attack surface for malicious actors. Despite advancements in cyber security frameworks, many enterprises in Karnataka struggle with inadequate security measures, lack of employee awareness, and regulatory compliance challenges. The implementation of India’s Personal Data Protection Bill (PDPB) and global standards like GDPR further complicates the cyber security landscape, requiring businesses to adopt robust risk management strategies.

This research paper explores the key cyber security challenges faced by modern business enterprises in Karnataka, analysing prevalent threats, organizational preparedness, and mitigation strategies. By examining case studies of recent cyber incidents and evaluating existing policies, this study aims to provide actionable insights for businesses to strengthen their cyber security posture in an increasingly hostile digital environment.

2.OBJECTIVES OF THE STUDY

- The examine the current state of cybercrimes affecting business organizations in Karnataka.
- To explore the existing laws and legal frame works aimed at safeguarding business organizations operating on digital platforms.
- To identify the key challenges and issues encountered by businesses in Karnataka within the digital ecosystem.
- To propose practical solutions and preventive measures to mitigate cybercrimes targeting business organizations in the state.

3.REVIEW OF LITERATURE

With the rapid digitalization of business operations in Karnataka, cyber security has become a critical concern. Modern enterprises face evolving cyber threats, including data breaches, ransomware, phishing, and insider attacks. This literature review examines existing research on cyber security challenges faced by businesses in Karnataka, focusing on threat, regulatory compliance, and mitigation strategies.

An article on "cyber security: emerging challenges in the 21st century" authored by a group of people from the organization, discussed about the "security in the information age: the rise of cyber-attacks" the threat of a new age of cyber threats, cyber wars, and cyber espionage are on the rise, and with this, a whole new dimension arises in the realms of cyber security. A combination of technical expertise, law and an effective security infrastructure are the need of the hour towards achieving the objective of securing the information assets of the country. (Wipro Council for Industry Research - 2010).

Lack of Cyber security Awareness and Skilled Workforce - Research by the Indian Institute of Science (IISc, 2021) indicates a shortage of skilled cyber security professionals in Karnataka, despite high demand. Many businesses rely on outdated security frameworks, making them vulnerable (Patil & Desai, 2022).

Data Privacy and Compliance Issues - With the enforcement of the Digital Personal Data Protection Act (DPDPA), 2023, businesses in Karnataka struggle with compliance. A study by NASSCOM (2023) found that only 35% of SMEs in Karnataka have fully implemented GDPR-like data protection measures, exposing them to legal and financial risks.

Kutub Thakur [15] Cyber security was used interchangeably for the security of knowledge, where later it sees the human's role in the safety process, although formerly finding this an additional dimension. However, such a debate on cyber safety has major consequences, since it reflects on the ethical part of the whole society. Various systems and models have been developed to solve the problem of cyber security.

Julian Jang-Jaccard [16] Improving cyber security and protecting critical information infrastructure is important for the security and economic well-being of each country. Safer Internet (and protecting Internet users) have been an important part of the growth of new services and public policy.

Julian Jang-Jaccard [18] Improving cyber security and protecting critical information infrastructure is important for the security and economic well-being of each country. Safer Internet (and protecting Internet users) have been an important part of the growth of new services and public policy.

This literature review synthesizes key findings on cyber security challenges in Karnataka, providing insights for policymakers and businesses to strengthen cyber resilience.

4.RESEARCH METHODOLOGY

This study adopts a qualitative and descriptive research design based on secondary data to analyse cyber security challenges faced by modern business enterprises in Karnataka. The research relies on existing literature, reports, case studies, and industry publications to identify trends, threats, and mitigation strategies.

Sources of Secondary Data: Academic Journals & Research Papers on cyber security. Reports from Karnataka Cyber security Centre of Excellence (KCCE), MeitY (Ministry of Electronics and IT). Corporate Publications, News Articles & Case Studies covering cyber incidents in Karnataka.

5.LIMITATIONS OF THE STUDY

- Dependence on pre-existing data may lead to gaps in real-time threat analysis.
- Possible bias in industry reports favouring specific cyber security solutions.
- Lack of primary data (e.g., surveys/interviews) may limit depth in organizational-specific challenges.
- Lack of time constraints on in-depth study in the cyber security concepts.

6.CYBER SECURITY AN OVERVIEW

Cyber security is the practice of protecting systems, networks, and data from cyber threats such as unauthorized access, theft, damage, or disruption. It involves a combination of technologies, processes, and practices designed to safeguard digital assets and ensure the confidentiality, integrity, and availability of information.

Cyber security - The protection of computer resources and networks from unauthorised access, information disclosure, theft of data or disruption of activities conducted on the computer resource or network.

Cyber security standards - Techniques, best practices and/or certifications adopted to protection IT infrastructure from cyber threads. Cyber security standards are often adopted on a large scale to bring uniformity to industry on a national or global level.

Digital Literacy - Development of necessary skills for communication and accessing information in cyberspace and communicating with others

Threats - Malware, phishing, ransomware, DDoS attacks, and insider threats.

Hacktivists - A person who gains unauthorized access to computer files or networks in order to further social or political ends.

Data Breaches - A data breach is an incident in which sensitive, protected, or confidential data is accessed, stolen, or exposed without authorization.

Vulnerabilities - Weak passwords, outdated software, and unpatched systems.

Ransomware - Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks their device and demands a ransom in exchange for the decryption key or unlock code.

7.KARNATAKA INFORMATION TECHNOLOGY POLICY 2020-25

Introduction - The Karnataka IT Policy 2020-2025 aims to position Karnataka as the leading technology hub in India, driving innovation and economic growth. With a focus on emerging technologies, digital infrastructure, and inclusive growth, the policy seeks to create a robust ecosystem for start-ups, SMEs, and large tech companies. It emphasizes fostering innovation, skill development, and research, while promoting equitable technology access across urban and rural areas. Through targeted initiatives and incentives,

Karnataka aims to contribute significantly to India's trillion-dollar digital economy goal and solidify its status as a global IT leader.

Eligibility Criteria under KIT Policy 2020-25

- Information Technology (IT) involving the development, maintenance, and use of computer systems, hardware, software and networks for the processing and distribution of data. / or
- ITeS covering the entire spectrum of operations which exploit information technology for improving efficiency of an organisation as defined further under the "definitions" section,
- All legal entities operating in the ITeS industry or
- Any other IT/ITeS verticals / products covered under the National Information Technology Policy and related notifications as issued by the Govt. of India.
- The entity should have registered office in Karnataka as per the Companies act 2013 or the Entity should be registered as per the Karnataka shops and Commercial Establishment Act 1961.
- At least 50% of the entity's total qualified workforce should be based out of Karnataka, which should not include contract employees.

8.KARNATAKA CYBER SECURITY POLICY 2024

Introduction - The Karnataka Cyber security Policy 2024 aims to build a secure and resilient digital ecosystem in the state. It focuses on safeguarding critical infrastructure, promoting cyber security awareness, and fostering innovation in security technologies. The policy encourages collaboration between the government, industry, and academia, and provides incentives to cyber security start-ups. By strengthening data protection and implementing global best practices, Karnataka seeks to become a leading hub for cyber security, ensuring the safety and trust of its digital economy.

Eligibility Criteria under Cyber Security Policy 2024

- For Internship, Companies should be registered with KITS (Karnataka Innovation and Technology Society) or in Shops and Establishment Act and Companies can hire students from only Karnataka based academics institutes, universities, colleges, polytechnics, etc. to be eligible for this incentive.
- For Research and Development, the applicant should be a start-up working jointly in collaboration with an academic institution on cutting edge research in the cyber security domain. The start-ups has to be registered with KITS, based in Karnataka and should provide cyber security services, while the preference will be given to all academic institutions in Karnataka.
- For Reimbursement of Security audit fees the applicant should be a start-up registered with KITS. The Start-up who use the services of only CERT (Cyber Emergency Response Teams) in empanelled service providers for cyber security audit, incidence response activities.

Cyber Security Policy 2024 Pillars

- Building awareness - Cyber security awareness is vital due to rising cyber-attacks and increased digital adoption. Karnataka needs customized awareness campaigns to educate citizens on data privacy and online safety.
- Skill building - The demand for cyber security professionals in India is growing, but there's a shortage of skilled workers. Karnataka, with its top technical institutes, can close this gap by enhancing training and boosting the cyber security workforce.
- Promotion research and innovation – As a global innovation hub, Karnataka can lead cyber security R&D by leveraging its talent and infrastructure, advancing research in underfunded areas for public interest.

- Partnerships and collaborations for capacity building - Coordinated efforts are needed to combat cyber-attacks. Karnataka should equip government personnel and law enforcement with cyber security skills, creating robust frameworks to enhance its leadership in technology.
- Promotion of industry and start-ups - Karnataka can drive self-reliance in critical technologies by supporting its local cyber security industry and start-ups, sustaining its position as a global tech leader.

9.MAJOR CHALLENGES OF CYBER SECURITIES IN BUSINESS ENTERPRISES

In Karnataka, modern businesses face a multitude of cyber security challenges, including a surge in malware and ransomware attacks, especially targeting sectors like Professional Services, Government, and Education. These challenges are amplified by the rise of remote work, complex cyber-attacks, human error, and a shortage of skilled cyber security professionals. Additionally, the increasing reliance on AI and cloud technologies introduces new vulnerabilities and compliance issues.

Here's a more detailed look at the key challenges:

1. Rising Cyber-attacks:

- Malware and Ransomware: Karnataka has seen a significant number of malware and ransomware attacks, with daily incidents averaging in the thousands.
- Phishing and Social Engineering: These attacks, aiming to trick individuals into revealing sensitive information, remain a major threat.
- Supply Chain Attacks: Businesses are increasingly vulnerable to attacks targeting their suppliers and partners.
- Advanced Persistent Threats (APTs): These sophisticated attacks, often state-sponsored, can remain undetected for extended periods.

2. Internal Threats:

- Insider Threats: Intentional or unintentional actions by employees or contractors can lead to data breaches.
- Human Error: Mistakes like falling for phishing scams or misconfiguring security settings can create vulnerabilities.

3. Technological Challenges:

- Cloud Security: The shift to cloud computing introduces new risks related to data storage, access, and management.
- IoT and Endpoint Security: The proliferation of internet-connected devices creates more entry points for attacks.
- AI and Automation: While AI can enhance security, it also presents new vulnerabilities that attackers can exploit.
- Data Sprawl: The vast amount of data generated by AI and other technologies can be difficult to manage and secure.

4. Skills Gap and Cost:

- Cyber security Skills Shortage: There is a growing demand for skilled cyber security professionals, making it difficult for businesses to find and retain qualified personnel.
- High Costs: Implementing and maintaining robust cyber security measures can be expensive, particularly for small and medium-sized businesses.

5. Regulatory Compliance:

- Data Privacy Laws: Businesses need to comply with various data privacy regulations, adding to the complexity of cyber security.
- Industry Standards: Meeting industry-specific security standards adds another layer of compliance.

6. Other Challenges:

- Remote Work: Remote work setups can introduce new security risks if not properly managed.
- Lack of Awareness: Many businesses lack adequate awareness about the potential risks and how to mitigate them.
- Third-Party Risks: Vulnerabilities in third-party systems can expose a business to attacks.

MEASURES TO OVERCOME CYBER SECURITY CHALLENGES IN KARNATAKA

- Invest in cyber security awareness training**:** Educate employees about the risks and best practices.
- Implement robust security protocols: This includes firewalls, intrusion detection systems, and regular security audits.
- Strengthen cloud security measures: Ensure data is encrypted, access is restricted, and security protocols are followed.
- Develop incident response plans: Be prepared to handle cyber-attacks effectively.
- Stay updated on emerging threats: Keep abreast of new attack vectors and technologies.
- Consider hiring a cyber-security consultant: Seek expert advice to assess vulnerabilities and implement appropriate solutions.
- Collaborate with other businesses and organizations: Share information and best practices to enhance collective security.

10.APPLICABILITY OF CYBER SECURITY POLICIES OF KARNATAKA

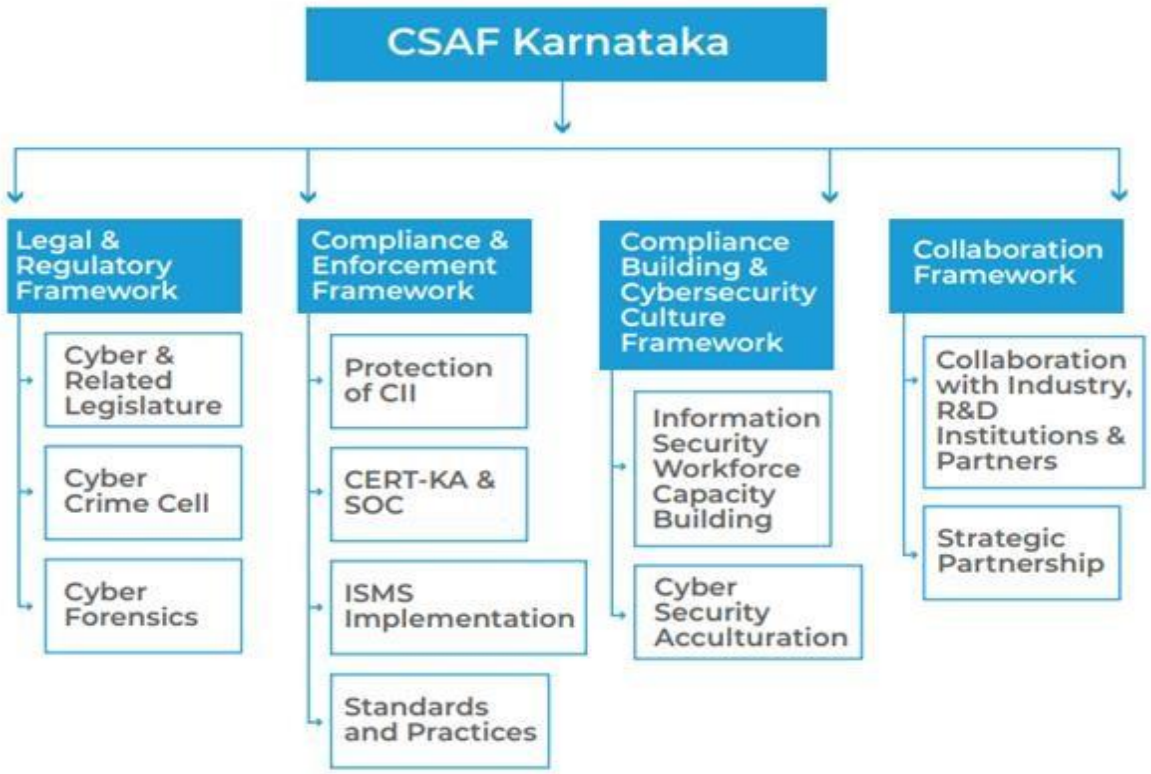
This policy is in line with National Cyber Security Policy of India and applicable to all Government Departments and Government agencies of the state of Karnataka. It covers protection of information assets such as Hardware, System Software, Application Software, data, Databases, Network infrastructure and electronic Services of the Departments and agencies of the State Government.

This policy is applicable to private Agencies, third parties, contractors, outsourced partners, and personnel who are associated with departments and agencies of Karnataka Government in providing IT and IT enabled services. This Policy applies to Central Infrastructure and Personnel who provide Services to the Karnataka Government either on specific deputation or by specific tasking.

Nothing in this Policy contravenes any applicable law of the Government of India or Government of Karnataka nor the policies of respective Governments. However, if any conflicts suspected, it must be brought to the notice of the Department of Personnel Administration and Reforms (e-Gov), Government of Karnataka immediately

11.CYBER SECURITY ARCHITECTURE FRAMEWORK

The Cyber Security Architecture Framework of Karnataka (CSAF-KA) defines the overall ambit of the Cyber Security related Agencies in Karnataka. The Cyber Security Architecture of Karnataka (CSAF-KA) will be executed by DPAR (e-Governance). The major components that constitute the CSAF-KA are: (a) Legal & Regulatory Framework (b) Compliance and Enforcement Framework (c) Capacity Building and Cyber security Culture Framework (d) Collaboration Framework The Cyber security Policy Framework holds several other frameworks that are intended to provide a holistic and complete solution the cyber security threat.



KARNATAKA CYBER THREAT REPORT 2025

Seqrite, the enterprise arm of Quick Heal Technologies Ltd., a global cyber security solutions pro, has unveiled its Karnataka Cyber Threat Report 2025, offering an in-depth analysis of the cyber threat landscape in one of India's most digitally advanced states. The report reveals that,

- Karnataka recorded 1.78 million ransomware detections, with an average of 4,887 attacks daily
- The state contributed 4.3% of India's total malware detections and 9% of national ransomware incidents
- Bengaluru topped the list of affected cities in Karnataka, with 4x higher malware detection rates than the state average.
- Professional services face the highest number of attacks, followed by government and education sectors
- Telegram based threat actors launched daily attacks on government portals, hospitals, and educational institutions, including defacements and DDoS (Distributed Denial-of Service) disruptions.

Karnataka Cyber Threat Report also highlights how attackers exploited election cycles, financial year-end activities, and festive seasons to launch targeted campaigns. For example, phishing campaigns surged during the March-April 2024, possibly due to the elections that were scheduled around that period. Similarly, ransomware attacks on BFSI (Banking, Financial Services & Insurance) institutions peaked during tax filing periods in July 2024. Festive seasons saw scams targeting students and job seekers through fake admission and hiring portals.

Karnataka Cyber Threat Report also highlights how attackers exploited election cycles, financial year-end activities, and festive seasons to launch targeted campaigns. For example, phishing campaigns surged during the March-April 2024, possibly due to the elections that were scheduled around that period. Similarly, ransomware attacks on BFSI (Banking, Financial Services & Insurance) institutions peaked during tax filing periods in July 2024. Festive seasons saw scams targeting students and job seekers through fake admission and hiring portals.

The release of Karnataka Cyber Threat Report 2025 serves as a wake-up call for organizations across industries to prioritize cyber security as a core business function rather than an afterthought. By leveraging comprehensive cyber security solutions from Quick Heal and its enterprise brand Seqrite, which are designed to simplify IT security management while ensuring compliance with national data protection laws, individuals and businesses can build resilient defences against evolving cyber threats.

12.FINDINGS FROM THE STUDY

- Karnataka, being India's IT and start-up hub, faces a high frequency of cyber-attacks, including ransomware, phishing, and data breaches.
- As per the trustworthy report of Karnataka accounted for 4.3% of total malware detections i.e. 11.46M out of 266.67M and 9% total malware ransomware detections i.e. 1.78M out of 19.85M in India (Cyber Threat Report 2025).
- Bengaluru-based enterprises (especially SMEs and start-ups) are prime targets due to rapid digitization with inadequate security measures.
- Reports from Karnataka Cyber Crime Police indicate a 30% YoY rise in cyber fraud cases, including financial scams and corporate espionage.
- Cloud security gaps due to rapid adoption of cloud services without proper encryption and access controls.
- Phishing & social engineering attacks remain dominant due to low employee cyber security awareness.
- Supply chain attacks (e.g., third-party vendor breaches) are a growing concern for Karnataka's IT industry.
- Karnataka has a strong Information Technology policy but there is a lack in effective implementation and awareness.

13.MAJOR SUGGESTIONS FROM THE STUDY

- As Industrialisation and Technology is developing, the same way crimes relates to the cyber security is also increases so it is necessary to organisations be aware of cyber-attacks.
- New start-ups are focusing more on earning profit and survive in the market but they won't focus much on protecting the organisations from cyber-attacks. So, protecting the organisations from cyber threats is having an equal importance like profit and survival.
- Adopting new and updated version of cyber protection software is more important now a days in business organisations.
- Government has to frame a strong Information and Technology policy and at the same time creating an effective awareness on cyber security is also an essence.
- Conducting an awareness programs and training sessions are more important to entrepreneurs and general public both from rural and urban areas.
- Effective and quick handling of cyber-attacks cases is very important to protect the organisations and public confidence from the cyber hackers.
- Strict and unbiased decision is necessary against cybercrime to avoid or reduced the cyber-attacks in business operations.

- Implementation of advanced technology to protect the organisations transactions and data security against cyber-crime along with providing an effective training programs.

14.CONCLUSION OF THE STUDY

The research will provide a comprehensive overview of cyber security threats in Karnataka's business sector, regulatory gaps, and best practices for risk mitigation, aiding policymakers and enterprises in strengthening cyber resilience.

Karnataka's enterprises face evolving cyber risks due to technological advancements and weak security practices. While large corporations have robust defences, SMEs and start-up's remain vulnerable. Strengthening regulatory compliance, employee training, and advanced threat detection will be crucial for cyber resilience.

Cyber security issues and challenges pose significant threats to business enterprises, impacting data integrity, financial stability, and reputation. As cyber threats evolve, organizations must adopt proactive, multi-layered security strategies, invest in advanced technologies, and foster a culture of cyber security awareness. Collaboration, continuous monitoring, and incident response planning are critical to mitigating risks and safeguarding business operations in an increasingly digital world.

15.REFERENCES

1) https://eitbt.karnataka.gov.in
2) National Cyber Security Policy 2013 – MeitY
3) https://journals.lww.com/amit/fulltext/2024/11010/a_systematic_review_on_cybersecurity_threats_and.1.aspx
4) https://cs-coe.iisc.ac.in/
5) https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022062/pdf
6) https://www.jetir.org/papers/JETIR2311342.pdf
7) http://ijeie.jalaxy.com.tw/contents/ijeie-v13-n2/ijeie-2021-v13-n2-p77-85.pdf
8) https://www.researchgate.net/profile/Ifeoluwa-Wada/publication/385525362 Security compliance and its implication for cybersecurity/links/672925162326b47637c7aeac/Security-compliance-and-its-implication-for-cybersecurity.pdf
9) DSCI. (2023). Annual Cyber Threat Report for Karnataka.
10) Kumar, R., & Sharma, A. (2022). Phishing Attacks in Bengaluru's SMEs: A Case Study. IJCS.
11) NASSCOM. (2023). Data Protection Compliance in Indian Enterprises.
12) KCCE. (2023). Cloud Security Risks in Karnataka's IT Sector.
13) Reddy, P., & Menon, S. (2023). Insider Threats in Indian Corporations. Cyber security Journal.
14) H. Suryotrisongko and Y. Musashi, ''Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective,'' in Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA), Kaohsiung, Taiwan, Nov. 2019, pp. 162–167, doi:10.1109/SOCA.2019.
15) Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15
16) Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

17) www.seqrite.com/india-cyber-threat-report-2025

18) Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.