Role Of IT Security In Ecological Sustainability – A Case Study On Indian Financial Sector, An OSINT Approach

Shiny John[1*], Dr. Binu Thomas[2], Teddy N. Alias[3], Aleena Ann Sibi[4]

[1*]Mar Athanasius College (Autonomous), Kothamangalam College P.O, Ernakulam Dist. Kerala, India 686 666 shinyjohnkp@gmail.com
[2]Marian College(Autonomous), Kuttikkanam P.O, Peermade, Idukki District, Kerala, India 685 531 binumarian@gmail.com
[3]Mar Athanasius College (Autonomous), Kothamangalam College P.O, Ernakulam Dist. Kerala, India 686 666 teddynalias@gmail.com
[4]Electronics and Communication Engineering, Rajagiri School of Engineering And Technology, aleenaannsb14@gmail.com

***Corresponding Author:** Shiny John
*Mar Athanasius College (Autonomous), Kothamangalam College P.O, Ernakulam Dist. Kerala, India 686 666 shinyjohnkp@gmail.com

ABSTRACT

In industry 4.0, the concept of stainable development has emerged as a critical endeavour for maintaining the ecological balance and survival of living beings. Lack of Ecological sustainability emphases the importance of maintaining a delicate balance between human activities and the natural world. Ecosystems undergo changes over time due to natural disturbances or human activities. Understanding the interplay between technological advancements and urbanization is crucial for addressing carbon footprints and identifying these impacts is vital for implementing sustainable practices and mitigating further damage to ecological balance. The emission of greenhouse gases produced by digital technology platforms and resources are known as digital carbon footprint. This study explores the principles, challenges and advancements in green cybersecurity also known as sustainable or eco-friendly computing. The research paper aims to delve into the role of IT security in ecological sustainability, exploring its significance, challenges and potential solutions in ensuring the preservation of ecosystems and biodiversity. This open source intelligence (OSINT) study will reveal how vulnerabilities in the IT infrastructure of Indian Financial Sector causes penetration which includes various kinds of malware attacks and increases carbon foot printing. It also divulges how a strongly protected IT infrastructure will precisely search for and promote the innovations that are possible by smart green technologies to avoid carbon emissions.

Keywords: *Ecological Sustainability, Digital Carbon footprints, Indian Financial Sector, OSINT, Vulnerability, Infrastructure penetration, Malware attack*

1. INTRODUCTION

Significance of ecological sustainability lies in its capacity to secure a healthy environment for all life forms, including humans. By fostering practices that sustain ecosystems and their resources, it aims to support ecological balance, resilience, and the stability of natural systems. This approach is crucial for safeguarding biodiversity, securing essential resources, and maintaining the overall health and well-being of the planet and its inhabitants for generations to come. Human activities have significantly impacted ecological balance, causing widespread alterations to natural systems and disrupting the delicate equilibrium within ecosystem. Human-induced actions that contribute to the release of greenhouse gases leads to global warming and climate change. These changes alter ecosystems, affecting species distributions, habitats, and the timing of biological events [1].

Preserving biodiversity, restoring ecosystems, reducing greenhouse gas emissions, and fostering sustainable practices are integral components of a comprehensive approach toward mitigating climate change while ensuring the long-term health and resilience of ecosystems. Technological advancements are crucial for overcoming limitations and enhancing the effectiveness of sustainability efforts. But the technological advancements also significantly influence carbon footprints. The carbon footprint concept refers to total amount of greenhouse gases, primarily carbon dioxide (CO2) and other carbon compounds, emitted directly or indirectly by individuals, organizations, events and services. Carbon footprint serves as a key metric for measuring the environmental impact of human activities. It quantifies the amount of greenhouse gas emissions associated with various processes, products, or services, providing a tangible measure of their contribution to climate change [2].

Green computing initiatives reduces the greenhouse gas emissions which are the significant contributors to climate change. By implementing energy-efficient technologies and practices the industries can substantially reduce its carbon footprint. Green computing drives technological innovation encourages the development of eco-friendly hardware, energy- efficient software, and sustainable data centre designs. Even though this fosters a culture of sustainability and promotes the adoption of cleaner technologies across industries, but the technological limitations pose challenges in achieving optimal energy efficiency and sustainability [3]. Vulnerabilities within infrastructure of green technology will raise significant threats to data security and operational stability which affects the ecological sustainability. These vulnerabilities include outdated software, weak authentication, unpatched security flaws, misconfigured systems, insufficient encryption, weak IoT security, inadequate monitoring and dependency on third-party services. Vulnerabilities which support the malicious actors to potentially exploit the infrastructure are the weak points of green computing technology infrastructure. This weakness affects various services. In the environment sustainability the threats associated with these vulnerabilities in the green computing technologies leads to increase in carbon foot printing [4].

In this work an OSINT case study is carried out based on Indian Financial Sector’s IT infrastructure to reveal how the vulnerabilities in the infrastructure affects the carbon foot printing in green computing.

2. OBJECTIVES

Green computing refers to the practice of designing, manufacturing, using, and disposing of IT resources in an environmentally responsible manner. It involves reducing the environmental impact of technology-related activities by implementing strategies that minimize energy consumption, resource utilization, and waste generation throughout the lifecycle of computing devices and systems. Green computing emphasizes energy efficiency, resource optimization, recycling and the adoption of eco-friendly materials and technologies in hardware and software design, data centres and computing operations. The ultimate goal of this work is to identify how to implement a more environmentally sustainable and energy- efficient computing ecosystem and to implement this sustainable ecosystem how the security of IT infrastructure plays a pivotal role [5].

Information Technology security plays a pivotal role in the sustainability of environment. It protects the IT infrastructure by promoting the responsible use of technology and addressing the emerging challenges in the digital landscape. Security of such digital infrastructure that supports environmental sustainability initiatives is very essential to maintain the ecological system [6]. This may include the infrastructure that monitor and manage generation of renewable energy, water control systems, waste monitoring networks, and smart grid etc. By safeguarding the authenticity and accessibility of these systems, the infrastructure security helps in preventing the interruptions that could weaken the efforts of sustainability that leads to harm the environment. Green computing practices focus on optimizing hardware, software, and data centre operations, leading to reduced energy consumption which lowers carbon emissions, lessening the environmental footprint associated with energy production [7]. The study tries to identify and prove that why the increasing implementation of green technology devices and environmental monitoring systems demand strong IT security. As the environmental sustainability heavily relies on data security, collection of data, it’s analysis and sharing, the work attempts to reveal that the green technology devices that are highly secure are less threatened against attacks and prevents unauthorized accessing and steeling of data which otherwise may compromise their functionality causing increase in carbon foot printing
[8].

As renewable energy systems in green technologies have become more interconnected and dependent on digital infrastructure, the security of information technology has become crucial in mitigating associated risks. The aim of the study is identifying and exposing the risks associated with the vulnerabilities in green technologies and thus trigger an eye opening to the importance of protecting these technologies from the threats associated with the vulnerabilities such as ransomware attacks or unauthorized control and thus preserves public trust in their sustainability benefits and ensures their unfailing operation by preventing interruptions [9].

The objective of this work is to divulge the role of IT security in green technology to reduce the carbon foot print and support environmental sustainability. With the vulnerability case study in Indian Financial sector, using OSINT, the work addresses how much security risks exists there in their infrastructure which affects carbon foot printing and reveals the essentiality in protecting the critical infrastructure for securing the environmental data, nurturing the sustainable development of technologies and promote awareness regarding the importance of IT security in green computing among the environmental community [10].

3. METHODOLOGY

For a specific intelligence purpose, when publicly available information is gathered, evaluated, and analyzed, it is known as open source intelligence (OSINT). As the financial sector has huge amount of sensitive information stored in their IT infrastructure which are mostly vulnerable to data breaches through OSINT by malicious actors. Even in preventing or detecting financial crime, open source intelligence plays a pivotal role [11].

The financial sector has faced IT infrastructure attacks including data breaches, malware attacks targeting customer data and financial systems. Even after adhering to cybersecurity regulations and guidelines issued by the Reserve Bank of India (RBI), the study proves that security is still a challenge for financial entities and requires continual improvements in security measures and compliance frameworks. The intelligence can be collected about behaviour, reputation and online activities of individuals or organisations and will be gathered using various tools and the can evaluate based on specific risk indicators relating to financial crime. The openly available sources like public service hosts, exposed IT infrastructure and social media are targeted for information collection [12].

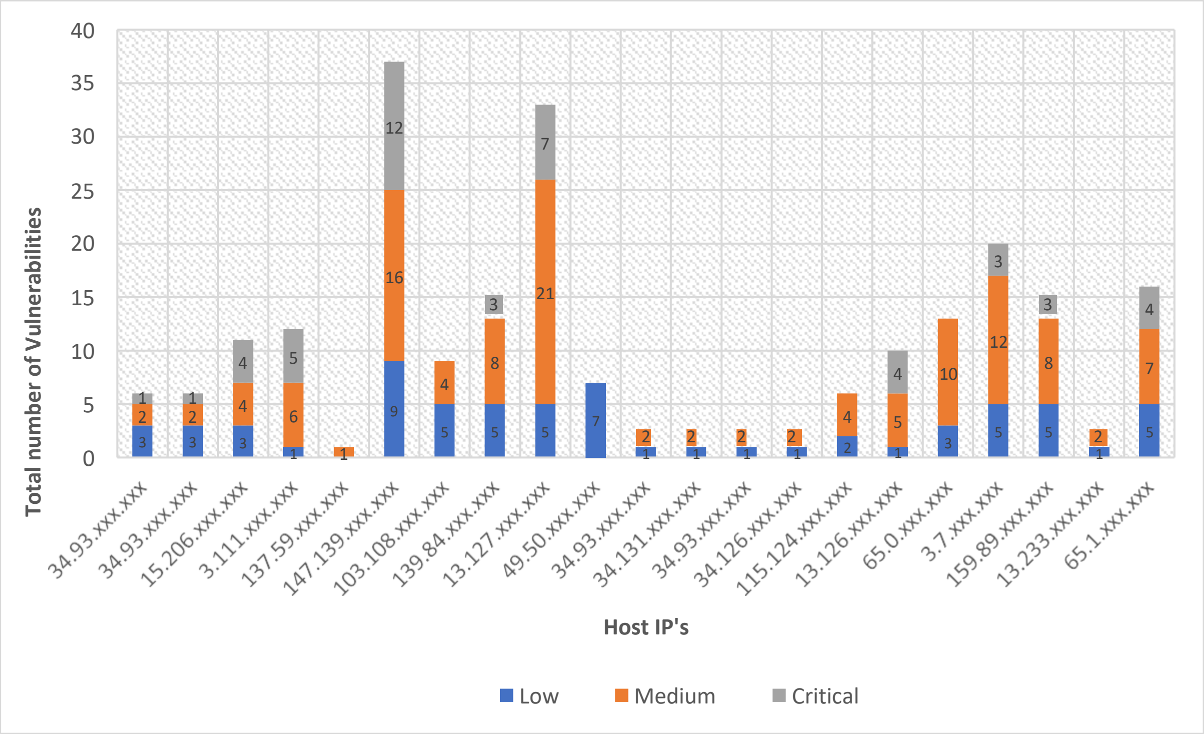
The case study based on “Role of IT Security in Ecological Sustainability” has an exact and detailed methodology. An intelligence gathering and analysis framework, SpiderFfoot, is used for this OSINT work. It’s ability to gather intelligence from publicly available sources has become a keystone in fortifying digital defences. Among the arsenal of tools and frameworks designed for this purpose, SpiderFoot stands as versatile intelligence gathering frame work that serves as a beacon in the quest for digital reconnaissance. It is free and open source and its flexibility makes it accessible to a wide range of users. It contains many modules that are used for information gathering. It integrates with just about every data source available and utilizes a wide range of methods for data analysis. From a technical point of view SpiderFoot typically employ various phases of operations: In the first phase through data collection process, the public host IP enumeration is done focusing the Indian financial sector. It initiates data gathering from a wide array of publicly available user end point services including search engines, social media platforms, public databases, websites, e-commerce and e-bank portals, DNS records, WHOIS information and more. It uses various techniques like web scraping, API interactions and querying public repositories for collecting IP’s. In the next phase, once data is collected, it undergoes parsing and cleaning processes. Irrelevant or redundant data is out while essential information is organized for further analysis. SpiderFoot's algorithm correlates and analyses the collected information. It identifies patterns, establishes relationships and connects disparate data points to create a comprehensive view of the target entity's digital presence. Algorithms may involve link analysis, pattern recognition and data clustering. The frame often employs visualization techniques to present the analysed data in graphical formats such as graphs, charts and maps. Visual representations aid in understanding complex connections and patterns quickly. SpiderFoot assesses the significance of the discovered data points, assigning priorities based on potential risks, threats, or vulnerabilities. This prioritization helps investigators focus on critical areas that require immediate attention. And finally, the framework is used to exhibit the detailed reports to the IT security professionals, investigators or analysts offering insights on the possibility of generation of carbon foot print due to the insecurity in IT infrastructure [13].

As it is found that the data accumulated from the reconnaissance process of the first phase by itself was not as useful enough, an addition to this, also decided, an exhaustive analysis process also had to be interpreted in the primarily collected data, to elaborate the firstly derived evidences. After the initial phase of reconnaissance, the frame work used Nmap, a free powerful network security auditing tool for Port Scanning & Network Exploration. Nmap also comes with various scripts that detects security weaknesses. Its functionality extends beyond standard port scanning, delving into the realm of vulnerability assessment through the execution of NSE (Nmap Scripting Engine) scripts [14]. For this OSINT study a White Hat level approach has been carried out among a set of randomly selected Indian Financial organisations. From the publicly accessed sources it generated meaningful intelligence of hundred IP’s. It explored the target’s deep network information like ports available, their status, web servers used and their versions, services running and the operating systems running. In this work the open source intelligence give us insights into how an organization’s infrastructure is structured, what all hardware and software services they offer and thus exploring the level of threats which indirectly generate carbon foot printing, thus breaking the ecological sustainability [15].

4. RESULT

In this work a complete life cycle of intelligence gathering approach is carried out among one of the most critical infrastructures of India, the Financial sector, as to analyse the security weakness in the IT infrastructure which may lead to cyber-attacks. The case study reveals the importance of robust cybersecurity measures, regular risk assessments, implementation of advanced security technologies, employee training and the maintenance of regulatory compliances.

The open source intelligence gathering was carried out based on hundred randomly chosen host IP’s of Indian Financial sector. Initially in the reconnaissance phase targeting relevant open sources, openly existing information were collected based on the above hundred IP’s. As the whole process of intelligence gathering is triggered from the reconnaissance stage, the initial process plays a prominent role in the investigation process. After the initial phase of OSINT using one of the plugin modules of Spiderfoot, NMAP, we came to a conclusion that among those hundred IP’s, twenty one IP’s of Nationalised banks and Financial markets were found vulnerable to various attacks categorised under various CVE’s.



Threat impacts in Indian Financial Sector

CVE is a curated list of security vulnerability information that are catalogued and open to the public. These vulnerabilities, often discovered in software, hardware, or network infrastructures, are identified, documented, and made available to the public for reference, mitigation, and resolution. Each vulnerability in the CVE list is given a unique identification number, facilitating easier tracking and communication across the cybersecurity community and also given a threat impact score. Based on the threat impact the CVE's of the vulnerabilities encountered in the OSINT analysis of Indian financial sector are categorised into three levels: low, medium and critical. Vulnerabilities refer to weaknesses or flaws in systems, software, hardware, or processes that can be exploited by attackers. The threats existing within the infrastructure are potential risks and causes malicious activities that can exploit vulnerabilities and cause harm to systems, data, or networks. The threat actors exploit vulnerabilities with various determinations like illegal access, data theft, interruption or for monetary benefits. In the above case study various threats encountered in the IT infrastructure of Indian financial sector are MITM attacks, DDoS, RCE etc. which all leads to unauthorised access of resources, data loss, ransomware attack, delay or unavailability of resources, server security feature bypass, excessive memory consumption, server crash, leak of potentially sensitive information, DNS cache poisoning, redirection of users to a wrong web sites, resource unavailability, bypassing of configured access control restrictions and hackers can penetrate into users accounts to get financially by stealing funds or purchasing items with stolen credit cards.

The case study reveals that due to security vulnerabilities in the IT infrastructure, the Indian financial sector is encountering with various security threats that affects the functioning of financial institutions. The impact of the above attacks extends beyond immediate financial losses, encompassing reputational damage, regulatory scrutiny, customer trust erosion, and operational disruptions. Recovering from the IT infrastructure attacks requires significant resources, man power, time and effort. After the IT infrastructure attack, the sector may need to recover operations potentially and that may require more man power and excess working hours to escape from the deadlock situation, increases the workload on other systems, and may disrupt the normal business operations and thus will escalate the energy usage and carbon emissions. Hence the OSINT study proves that the failure in IT security measures indirectly affects the carbon foot printing which interrupts the ecological sustainability. Strong IT security prevents cyberattacks, data breaches, or ransomware attacks that could disrupt operations, compromise data, or manipulate carbon footprint calculations and could undermine the accuracy of sustainability initiatives and reporting.

5. CONCLUSION ANDRECOMMENDATIOS

The OSINT work on the security of Indian financial sector's IT infrastructure proves that the Indian financial industry needs to be evolved in its security measures by preventing outside and inside threats to protect the infrastructure for safeguarding sensitive financial data not only to ensure the trust of customers but also to control carbon foot printing to maintain the ecological sustainability. Service breakdowns or downtime in banking IT infrastructure, though not directly

related to carbon footprint, indirectly impact it. When systems fail or require maintenance, banks may need to redirect operations, potentially increasing the workload on other systems, thereby escalating energy usage and carbon emissions. The higher the level of energy consumption, the higher the carbon footprint and which in effect collapses the ecological sustainability. Robust IT security measures protect against cyber threats, malware, and data breaches that could disrupt eco-friendly operations. Ensuring the security of systems involved in green computing practices mitigates the risks of disruptions and data loss. Strong security measures facilitate the adoption of sustainable IT technologies that improve energy efficiency and reduce the environmental impact on the implementation of green technology.
The work " Role of IT Security in Ecological Sustainability – A case study on Indian Financial Sector, an OSINT Approach" reveals how import is the role of IT security in ecological sustainability. It also proves that recognizing interdependence between information technology and ecological sustainability is crucial for developing holistic strategies that addresses the above challenges. IT security in green computing ensures continuity in sustainability efforts by safeguarding against disruptions. This study helps in implementing secure green technology initiatives that controls the energy consumption and environmental impacts, allowing for consistent and accurate carbon foot printing that maintains the environmental sustainability.

ACKNOWLEDGEMENT

The authors of the paper would like to express their gratitude to those who supported them for gathering information. The authors are also thankful for the computing resources provided by Mar Athanasius College (Autonomous), Kothamangalam, Kerala.

REFERENCES

1. Feroz, A. K., Zo, H., & Chiravuri, A. (2021). Digital transformation and environmental sustainability: A review and research agenda. Sustainability, 13(3), 1530.
2. Shi, S., & Yin, J. (2021). Global research on carbon footprint: A scientometric review. Environmental Impact Assessment Review, 89, 106571.
3. Paul, S. G., Saha, A., Arefin, M. S., Bhuiyan, T., Biswas, A. A., Reza, A. W., ... & Moni, M. A. (2023). A comprehensive review of green computing: Past, present, and future research. IEEE Access.
4. Sharma, P., & Dash, B. (2022). The digital carbon footprint: Threat to an environmentally sustainable future. International Journal of Computer Science & Information Technology (IJCSIT) Vol,14.
5. Sharma, D. K., Gupta, K. D., & Dwivedi, R. (Eds.). (2022). Green Computing in Network Security: Energy Efficient Solutions for Business and Home. CRC Press.
6. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
7. Rani, R., Kumar, S., Kaiwartya, O., Khasawneh, A. M., Lloret, J., Al-Khasawneh, M. A., ... & Alarood, A. A. (2021). Towards green computing oriented security: A lightweight postquantum signature for IoE. Sensors, 21(5), 1883.
8. 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.
9. Cavelty, M. D. (2007). Critical information infrastructure: vulnerabilities, threats and responses. In Disarmament Forum (Vol. 3, pp. 15-22). UNIDIR.
10. Panagariya, A. (2022). Digital revolution, financial infrastructure and entrepreneurship: The case of India. Asia and the Global Economy, 2(2), 100027.
11. Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of osint. Wireless Communications and Mobile Computing, 2022.
12. Panagariya, A. (2022). Digital revolution, financial infrastructure and entrepreneurship: The case of India. Asia and the Global Economy, 2(2), 100027.
13. Yaworski, P. (2019). Real-world bug hunting: a field guide to web hacking. No Starch Press.
14. Calderon, P. (2021). Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips. Packt Publishing Ltd.
15. Bazzell, M. (2016). Open source intelligence techniques: resources for searching and analyzing online information. CreateSpace Independent Publishing Platform.