IJMSERH

International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

Volume 12, Issue 2, April-June 2024

Impact Factor: 9.274

ijmserh@gmail.com

www.ijmserh.com

International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

National Public Data Breach

Sudheer Kolla

Unisoft Technology Inc, Aubrey, Texas, USA

ABSTRACT: The 2024 National Public Data breach is one of the largest cyber-attacks ever; it affected over 2.9 billion individuals in the United States, the United Kingdom, and Canada. The attack involved private information such as names, social security numbers, addresses, and telephone numbers, which put millions of people at risk of identity theft and financial fraud. The "USDoD" hacker successfully intruded on the weak encryption system, which went undetected for over four months. This article will concentrate on the time of the hack, the motives behind it, and its extensive implications for persons, institutions, and regulatory systems. It mainly deals with the security lapse regarding National Public Data and loopholes in the regulatory mechanism, which is why such a mega hack became possible. The article further recommends how such incidences could be avoided in the future, including advanced algorithms for encryption, two-factor authentication, and international measures against cybersecurity. By discussing what could be learned from this breach, this study underlines the importance of proactive cybersecurity and international cooperation in countering the new threat constituted by data breaches.

KEYWORDS: Cybersecurity, Data Privacy, Data Encryption, Identity Theft

I. INTRODUCTION

The ever-increasing usage of digitized data at organizations has redesigned how they store, work, and handle information. These digital technologies allow businesses to make their customer experience far superior and enable smoother operations, but they open the door to some unprecedented challenges: cybersecurity [1]. The National Public Data Breach of 2024 has shown both the risks of large-scale data aggregation and the disastrous consequences of not securing sensitive information. It has been widely regarded as one of the largest data breaches in history, affecting over 2.9 billion people in the United States, the United Kingdom, and Canada, whose sensitive personal information, including Social Security numbers, home addresses, and phone numbers, has been exposed and is easy for cybercriminals to use in fraud and identity theft [2].

This breach occurred in December 2023 but was not detected until April 2024. At its discovery, the data was being sold on the dark web by the hacker in question, known as "USDoD," for $3.5 million in ransom [2]. The delay in detection indicated some critical failures within the threat-monitoring system at National Public Data and its inability to implement proactive security. These shortfalls not only scale up the breach but also magnify the long-term damage caused to the victims and stakeholders.

The paper closely looks at the breach to determine the root causes of poor encryption protocols, human error, and supply chain vulnerabilities. It also investigates the legal, regulatory, and economic consequences of the breach that finally brought National Public Data to its knees. It provides recommendations to organizations and policymakers with actionable steps that may be taken to mitigate similar cybersecurity-related risks in the future. The National Public Data Breach serves as a strong example, showing how these systemic sets of vulnerabilities in data protection led to significant harm and point to the imperative of more substantial global standards and increased cybersecurity practices.

II. BACKGROUND OF THE NATIONAL PUBLIC DATA BREACH

The National Public Breach started in December 2023, when a hacker took advantage of several vulnerabilities in National Public Data's infrastructure and gained unauthorized access to sensitive information [2]. As a key infiltrator of public and private information in America, the United Kingdom, and Canada, the corporation housed a diverse pool of individual information, providing a flawless target for hackers [2]. In contrast to claims of having robust security structures, a period of almost four months elapsed between when the attack happened and when it could be detected. That four-month period provided a window for a hacker to download and manipulate information with no restrictions at all [3]. By April 2024, hacker alias "USDoD" publicly posted information about publicly advertised datasets for resale in the dark web marketplace, providing a $3.5 million ransom in cryptocurrencies for not publicly disclosing it [2].

International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

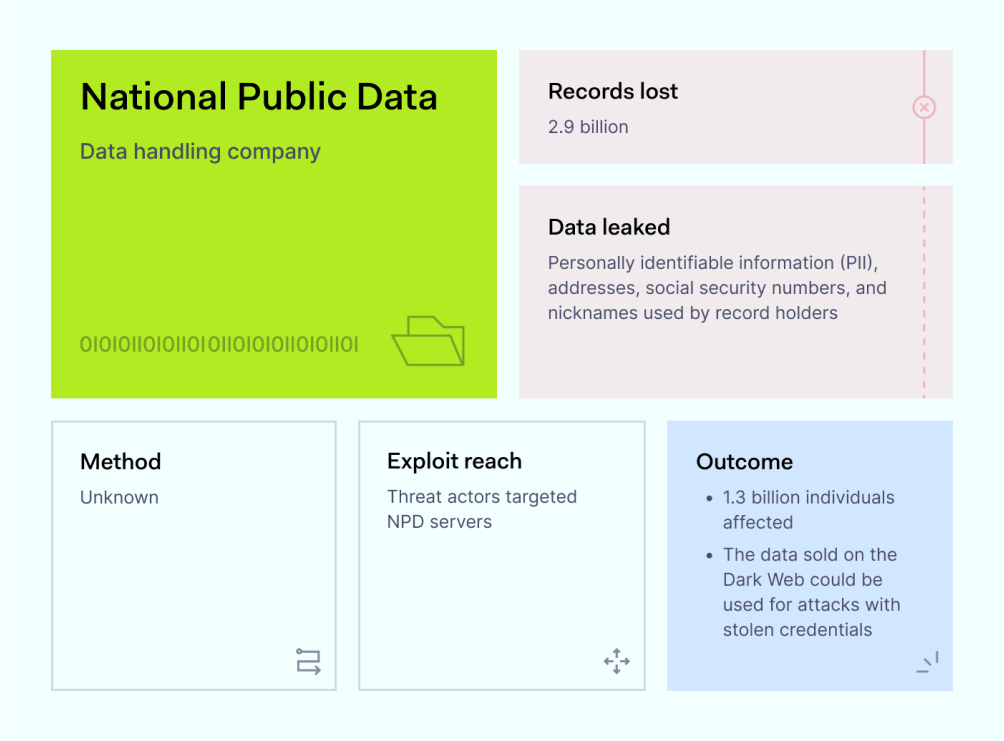

Figure 1: 2024 biggest data breach, involving records with diverse personally identifiable information, social security numbers, historical addresses, and nicknames used by record holders (Source: https://nordlayer.com/blog/data-breaches-in-2024/)

The information compromised included sensitive individual information such as full name, social security, contact phone numbers, and residential addresses [2, 3]. That pool of sensitive information facilitated ideal environments for hostile operations such as identity leakage, financial scams, and bulk phishing operations. For many, the attack started immediate financial peril and long-term vulnerabilities towards hackers.

The attack investigation showed systemic failures in National Public Data's information security structures. National Public Data utilized outdated security structures for scrambling, and a significant portion of information happened to spread unscrambled and accessible for exploiters. To make matters worse, National Public Data subcontracted a portion of its information processing, most with no security structures for securing information. Those vulnerabilities in its value chain presented added attack channels [3].

The breach initiated widespread criticism, lawsuits, and investigations initiated at national and state levels. National Public Data's inattention in dealing with the incident and its aftermath translated to enormous financial loss and loss of public trust and confidence [2]. In 2024, the corporation collapsed, one of the largest collapses in a corporation with a cybersecurity break in U.S. history.

III. CAUSES AND VULNERABILITIES OF THE BREACH

With the advancing technology, there has been an emergence of common cyber risks [4], which many companies, such as National Public Data, have been susceptible to. Although such cyber risks are dynamic, some common ones have thrived increasingly, such as data malicious breaches and unintentional disclosure, as presented in Figure 2.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

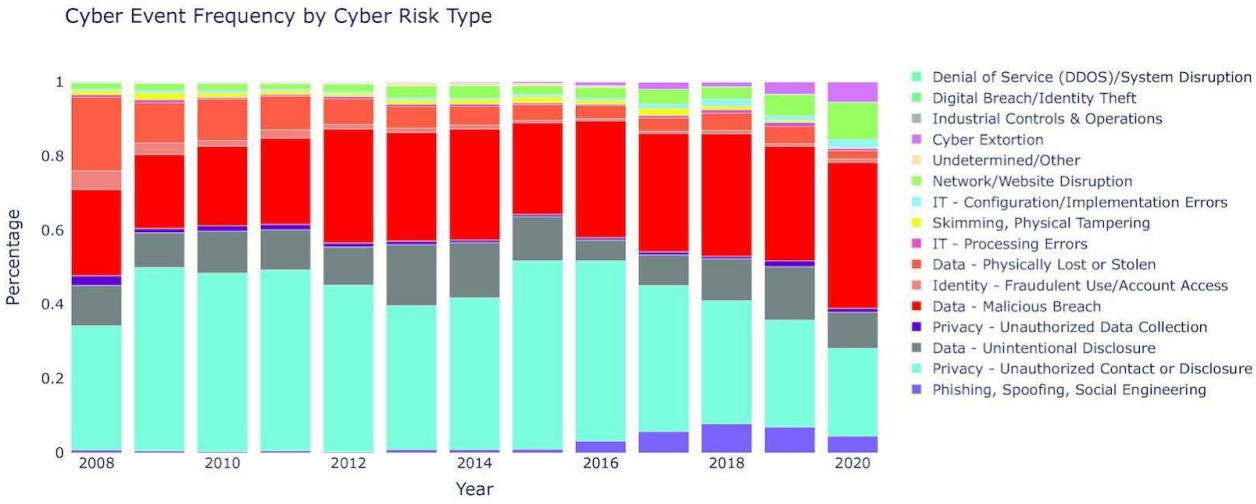

Figure 2: Frequency of cyber risk types (Source: https://doi.org/10.1093/cybsec/tyac016)

The National Public Data breach stemmed from technological weaknesses [5], human errors [6], and system weaknesses in the company's operations, which are also common issues of data breaches in most companies, as shown in Figure 3. One of the key factors in the breach involved National Public Data's use of outdated encryptions [2]. Contemporaneous encryptions, such as AES-256, have strong protocols designed to secure and protect sensitive information from unauthorized access [7]. National Public Data failed, however, to use such controls thoroughly, and large parts of its dataset remained unencrypted [3]. That lack of security left it remarkably simple for its adversary to extract and use sensitive information with little in its path.

Another key weakness in its operations involved its failure to detect its breach in a timely manner. Sophisticated persistent-threat hackers such as "USDoD" survive by abusing companies with poor threat-detection programs in their networks. National Public Data lacked real-time intrusion detection, and therefore, the hacker operated in its networks undetected for over four months [2]. That extended access facilitated its hacker to access enormous volumes of information and sell them on its dark web long before its leak was discovered.

Human fallibility compounded the leak, too. In investigations, the workers in National Public Data failed in cybersecurity protocol training, and the vulnerability to social engineering techniques, such as sending them a phishing message, saw them providing their hacker with its first footprint in their system [2]. Empirical studies have long confirmed that in successful cyberattacks, there is an increasing number of data breaches linked to human errors, either by employees or third parties who unintentionally trigger data breaches [8].

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

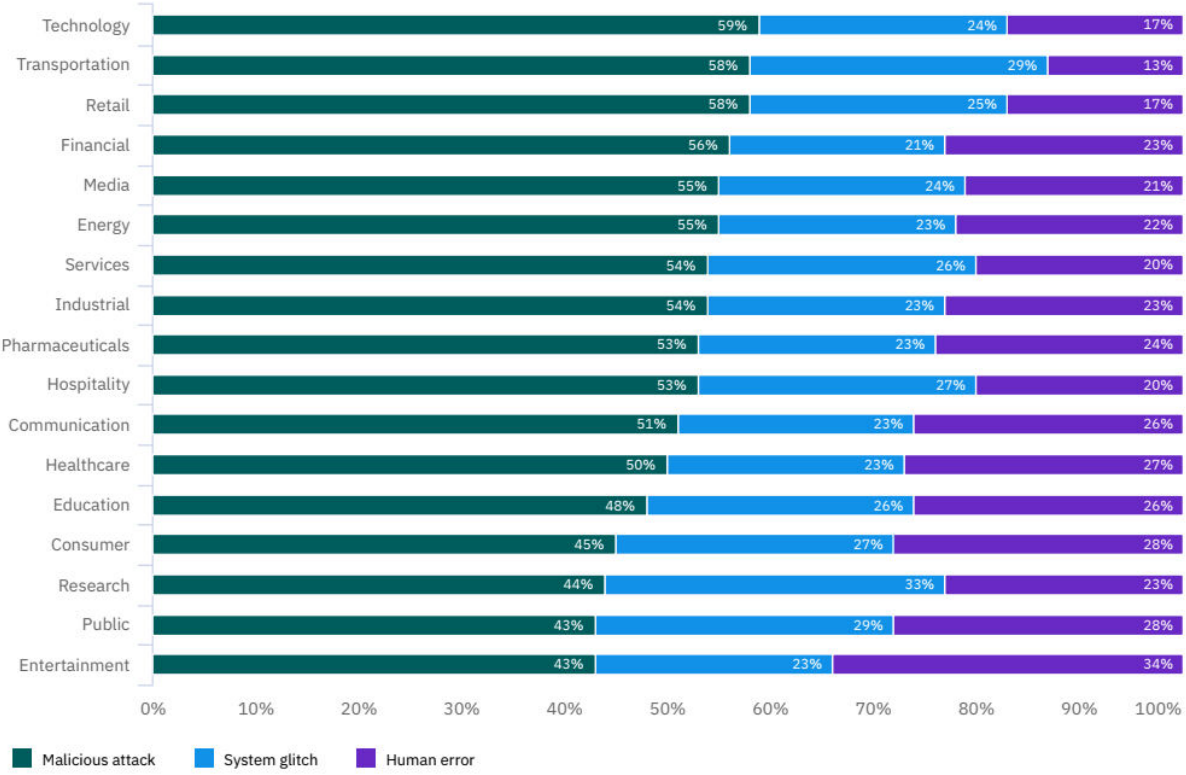

Figure 3: Common causes of data breach in different industries(Source: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf)

Supply chain vulnerabilities also contributed to the attack. National Public Data subcontracted its processing and administration of its information to external providers, most of whom did not have minimum security standards for cybersecurity [2, 3]. By default, such providers opened new avenues for the hacker, and it became even more challenging for the entity to safeguard its networks. Supply chain vulnerabilities have increasingly become widespread in current cybersecurity networks, with a tendency to amplify the level of vulnerability for entities that use external service providers [9].

Impacts of the National Public Data Breach:

The consequences of National Public Breach spilled over into individual, organizational, and government sectors. For citizens, the breach revealed sensitive information, and citizens encountered financial fraud and identity theft [2]. Victims encountered unauthorized transactions and accounts takeover, most with considerable financial loss. Besides, psychologically exhausting processes of fraud resolution and securing compromised accounts added a new source of tension and annoyance for citizens.

Organizations, most notably National Public Data, experienced irreparable loss in terms of loss of reputation. Public trust in the corporation's integrity in securing information resulted in a critical loss of confidence, which saw a fallout of investors and clients [2]. In terms of financial loss, lawsuits worth estimated billions of dollars entered the corporation, with citizens and companies demanding reparation for loss incurred through the breach [2, 3]. Reputational loss compounded financial loss, and National Public Data filed for bankruptcy mere months later when information about the breach entered public awareness. The economic consequence of the breach was felt in distinct spheres, such as finance, banking, and retail, where substantial disruption intensified [3]. In the health sector, fraud on claims and unauthorized access to medical records triggered operational issues [2]. Providers felt the need for additional investments in dealing with fraud cases, essentially postponing critical care for several periods [3].

At the national level, the attack shed new light on vulnerabilities in current frameworks for big data management in instances of enormous cyberattacks. The attack renewed talks in the USA regarding a uniform national cybersecurity environment. Those talks focused on heightened reporting requirements and severe penalties for nonconformity to

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

discourage future information security data breaches [10]. The National Public Data Breach increased vulnerabilities in current information system weaknesses and prompted private and public entities to reevaluate and redefine cybersecurity strategies [3]. Incidental repercussions of such a colossal attack stressed an urgency for strong defenses, proactive and effective controls, and worldwide coordination to minimize the chances of ever-evolving cyberattacks.

Legal and Policy Implications:
The National Public Data Breach uncovered enormous gaps in regulative and legal frameworks, triggering widespread legal actions and policy negotiations. National Public Data was sued for gross negligence in not protecting sensitive information [11]. Its failure to employ updated security controls and protocols, according to its accusers, amounted to a betrayal of trust and incurring billions of dollars in loss, for which it could settle a payment worth over $2 billion, putting a big financial burden on the ailing entity [11].

Aside from lawsuits, the breach uncovered enormous gaps in international information-protecting laws. In contrast, the European Union's GDPR mandates immediate reporting of a breach and imposing harsh penalties for noncompliance [12]; similar mandates in the United States and Canada at the incident were scattered at best. Governments in countries under impact have proposed enhancing cybersecurity controls and closing gaps in existing controls [3]. Proposals involved reporting a breach in a timeframe, enhancing penalties for non-conformity, and incentives for entities to utilize zero-trust security architectures. Zero-trust architectures depend on the "never trust, always verify" principle, with continuous authentication and strong access controls to minimize vulnerabilities [13].

The breach functioned as a wake-up call for governments and entities to prioritize harmonized regulatory and legal frameworks. By harmonizing information protection standards [1] worldwide and imposing stricter compliance regimes, governments can establish a safer cybersecurity environment capable of countering emerging cyberspace threats.

Recommendations for Prevention:
To prevent such a leak in the future, organizations will have an effective, multi-faceted cybersecurity practice in place. One of the first actions is having complex encryption protocols in place. End-to-end encryption, via protocols such as AES-256, keeps sensitive information safe during its life cycle [7]. Having such controls in place effectively lessens the opportunity for unauthorized access via compromised information in that such information cannot then be exploited. Organizations must also implement multifactor authentication (MFA) in all systems [14]. By having users authenticate through several forms of credentials, MFA introduces an added level of security, and unauthorized access is less likely [14].

Education and training for workers is crucial. Employee errors are prevalent in cybersecurity events, with social engineering and phishing scams consistently among untrained workers [15]. Organizations have to make cybersecurity training programs a high priority, training workers to detect and respond effectively to vulnerabilities. Programs must extend to third parties, too, with such parties having to comply with similar high-security standards in an attempt to stop vulnerabilities in the supply chain [9]. Contractual requirements and routine audits can secure compliance with such parties and mitigate external dependency-related risks.

Organizations must also invest in sophisticated threat detection and reaction tools. AI-powered monitoring tools can monitor suspicious activity in real-time [16], allowing for quick reactions to suspected breaches. Engaging with external cybersecurity professionals and participating in threat intelligence networks strengthens an organization's security even further in terms of fending off new and emerging threats.

Policymakers must then enact these organizational actions with increased controls through legislation and regulation. There will have to be reporting of data breaches, imposing extreme penalties for non-conformity, and placement of financial incentives for proactive security frameworks such as zero-trust frameworks [17]. Uniting technological innovation, training workers, and establishing strong controls through legislation and regulation can effectively counter future breaches and make sensitive information frameworks safer.

IV. CONCLUSION

The National Public Breach of 2024 is a painful reminder of vulnerabilities in big-data aggregation frameworks and the catastrophic consequences of poor cybersecurity protocols. With 2.9 billion-plus compromised, the breach revealed systemic vulnerabilities in encryption protocols, delayed threat discovery, and compliance environments. It wreaked

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

havoc in terms of identity theft and financial fraud, and it bankrupted National Public Data and crippled industries, including healthcare and finance.

The cause, impact, and legal consequences of the breach have been examined in this article, and it is a strong case for proactive cybersecurity protocols in an era when vulnerabilities in big-data aggregation frameworks can have such catastrophic consequences. The most critical vulnerabilities in encryption protocols, training for workers, and vendor compliance must be addressed, and compliance must be heightened for companies to obtain security protocols. Governments must have a role in harmonizing international compliance standards for protecting information, imposing stricter compliance protocols, and supporting fully-trusted security architectures.

The ramifications of this breach remind one of the imperatives for continuous awareness and collaboration in an era when cybersecurity threats become increasingly sophisticated and sophisticated tools become increasingly part of modern life. As technology continues to become an increasingly larger part of modern life, developing strong cybersecurity architectures is no longer a matter of preference but a necessity for protecting individual and organizational privacy, security, and trust.

REFERENCES

[1] G. P. Rodrigues, A. L. M. Serrano, A. N. L. Lemos, E. D. Canedo, F. L. L. Mendonça, R. O. Albuquerque, A. L. S. Orozco and L. J. G. Villalba, "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Revie," Data, vol. 9, no. 27, 2023.
[2] Microsoft, "National Public Data breach: What you need to know," microsoft.com, 2024. [Online]. Available: https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535. [Accessed 28 May 2024].
[3] CID, "Cybercrime Prevention Flyer: National Public Data Breach 2024," Army Criminal Investigation Division, 2024.
[4] G. A. P. Rodrigues, A. L. M. Serrano, G. F. Vergara, R. O. Albuquerque and G. D. Nze, "Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies," Future Internet, vol. 16, no. 6, 2024.
[5] M. Thakur, "Cyber Security Threats and Countermeasures in Digital Age," International Journal of Applied Science and Education, vol. 40, no. 1, 2024.
[6] H. Faotu, O. N. Asheshemi and E. T. Jeremiah, "Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures," Journal of Science and Technology, vol. 30, no. 1, 2024.
[7] A. Goel, H. Baliyan, S. Tyagi and N. Bansal, "End to end encryption of chat using advanced encryption standard-256," International Journal of Science and Research Archive, vol. 12, no. 01, 2024.
[8]IBM, "What is cybersecurity?," ibm.com, 2024. [Online]. Available: https://www.ibm.com/think/topics/cybersecurity. [Accessed 29 May 2024].
[9] R. K. Ray, F. R. Chowdhury and R. Hasan, "Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection," Journal of Business and Management Studies, vol. 6, no. 1, 2024.
[10] N. O. Miracle, "The Importance of Network Security in Protecting Sensitive Data and Information," International Journal of Research and Innovation in Applied Science (IJRIAS), vol. IX, no. VI, 2024.
[11] J. Gregory, "National Public Data breach publishes private data of 2.9B US citizens," Securityintelligence.com, 2024. [Online]. Available: https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/. [Accessed 28 May 2024].
[12] The European Data Protection Board, "Guidelines 9/2022 on personal data breach notification under GDPR," edpb.europa.eu, 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf. [Accessed 29 May 2024].
[13] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," Internet of Things, vol. 27, 2024.
[14] R. K. Mahmood, A. I. Mahameed, N. Q. Lateef, H. M. Jasim, A. D. Radhi, S. R. Ahmed and P. Tupe-Waghmare, "Optimizing Network Security with Machine Learning and Multi-Factor Authentication for Enhanced Intrusion Detection," Journal of Robotics and Control (JRC), vol. 5, no. 5, 2024.
[15] J. Olaniyan and A. A. Ogunola, "Protecting small businesses from social engineering attacks in the digital era," World Journal of Advanced Research and Reviews, vol. 24, no. 03, 2024.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

DOI: 10.15662/IJMSERH.2024.1202002

[16] J. K. Manda, "AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations," International Journal of Multidisciplinary and Current Educational Research (IJMCER), vol. 6, no. 2, pp. 333-340, 2024.
[17] A. Akinsanya, "Securing the Future: Implementing a Zero-Trust Framework in U.S. Critical Infrastructure Cybersecurity," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 10, no. 3, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

International Journal of Multidisciplinary and Scientific Emerging Research (IJMSERH)

Impact Factor: 9.274

ijmserh@gmail.com

www.ijmserh.com