Enhancing Security in IoT Networks: Investigating Novel Methods to Improve Security Protocols and Defences in IoT Environments

By ***Prof. Luca Rossi****,*

Professor of Distributed Edge Systems, Politecnico di Milano, Italy

Abstract:

The Internet of Things (IoT) has revolutionized the way devices interact and communicate, enabling unprecedented convenience and efficiency in various domains. However, the interconnected nature of IoT devices raises serious security concerns, as they are susceptible to a wide range of attacks. Enhancing security in IoT networks is crucial to mitigate these threats and ensure the integrity, confidentiality, and availability of IoT systems. This paper explores novel methods to improve security protocols and defenses in IoT environments. We discuss key challenges in securing IoT networks, such as resource constraints, heterogeneity, and scalability issues. Furthermore, we review existing security mechanisms and propose innovative approaches to address the evolving threat landscape. Our research aims to provide valuable insights and practical recommendations for enhancing security in IoT networks, ultimately fostering a safer and more secure IoT ecosystem.

Keywords: IoT, security, network, protocols, defenses, cybersecurity, IoT devices, threats, challenges, innovations.

I. Introduction

The Internet of Things (IoT) has emerged as a transformative technology, connecting billions of devices and enabling seamless communication and data exchange. From smart homes and wearable devices to industrial sensors and autonomous vehicles, IoT has permeated various aspects of our lives, offering unprecedented convenience and efficiency. However, the rapid

proliferation of IoT devices has also raised significant security concerns. The interconnected nature of these devices, combined with their often limited computational resources and diverse communication protocols, makes them vulnerable to a wide range of cyber threats.

Ensuring the security of IoT networks is paramount to protect against potential attacks that can compromise data integrity, confidentiality, and availability. Securing IoT environments poses unique challenges due to the scale and heterogeneity of devices, as well as the resource constraints under which they operate. Traditional security mechanisms are often insufficient to address these challenges, necessitating the development of novel methods and protocols to enhance the security of IoT networks.

This paper aims to investigate novel methods to improve security protocols and defenses in IoT environments. We begin by discussing the challenges inherent in securing IoT networks, including resource constraints, device heterogeneity, and scalability issues. We then review existing security mechanisms commonly employed in IoT systems, such as authentication, encryption, and intrusion detection systems. Subsequently, we propose innovative approaches and technologies to enhance the security of IoT networks, including machine learning for anomaly detection, blockchain for secure data exchange, and hardware-based security solutions.

By exploring these novel methods and technologies, this research seeks to provide valuable insights and practical recommendations for enhancing security in IoT networks. Ultimately, our goal is to contribute to the development of a safer and more secure IoT ecosystem, enabling the continued growth and adoption of IoT technologies across various domains.

II. Challenges in IoT Security

Securing IoT networks presents several unique challenges that differentiate them from traditional computing environments. These challenges stem from the inherent characteristics of IoT devices, including their resource constraints, heterogeneity, and the scale of deployment.

Resource Constraints: IoT devices are often constrained in terms of processing power, memory, and energy. This limits their ability to implement complex security mechanisms, making them susceptible to attacks that exploit these limitations. For example, many IoT devices lack the computational resources to support robust encryption algorithms, leaving data vulnerable to interception and tampering.

Heterogeneity of Devices: IoT ecosystems consist of a wide variety of devices with diverse capabilities, communication protocols, and security requirements. This heterogeneity makes it challenging to establish standardized security measures that can be applied uniformly across all devices. Moreover, managing and updating security protocols on such a diverse set of devices can be logistically complex.

Scalability Issues: IoT networks are characterized by their massive scale, with potentially millions of devices connected to a single network. This scale introduces challenges in terms of managing and securing such a large number of devices. Traditional security approaches may struggle to scale effectively to protect every device in the network, leaving vulnerabilities that can be exploited by attackers.

Addressing these challenges requires innovative solutions that can accommodate the resource constraints, heterogeneity, and scale of IoT networks. Next, we will explore existing security mechanisms commonly employed in IoT environments.

III. Existing Security Mechanisms

Despite the challenges, several security mechanisms have been developed and implemented in IoT environments to protect against various threats. These mechanisms aim to address key aspects of IoT security, such as authentication, encryption, and intrusion detection.

Authentication and Access Control: Authentication mechanisms are essential for verifying the identity of devices and ensuring that only authorized devices can access the network. Common authentication methods include password-based authentication, digital certificates, and biometric authentication. Access control mechanisms further enforce security by limiting the actions that authenticated devices can perform within the network.

Encryption: Encryption is crucial for protecting data transmitted between IoT devices and networks. It ensures that data remains confidential and cannot be intercepted or tampered with by unauthorized parties. Popular encryption algorithms used in IoT include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).

Intrusion Detection Systems (IDS): IDS are used to monitor IoT networks for suspicious activity and potential security breaches. IDS can detect anomalies in network traffic, unauthorized access attempts, and other indicators of a security threat. IDS can be implemented at the network level, the device level, or both, depending on the specific security requirements of the IoT environment.

While these existing security mechanisms provide a foundational level of security for IoT networks, they are not without their limitations. For example, traditional authentication methods such as passwords can be vulnerable to brute-force attacks, and encryption algorithms may be computationally intensive for resource-constrained devices. As such, there is a need for innovative approaches to enhance the security of IoT networks and address the evolving threat landscape.

IV. Novel Methods for Enhancing Security

To address the limitations of existing security mechanisms and mitigate the evolving threats to IoT networks, researchers and industry practitioners have proposed several novel methods and technologies. These innovative approaches leverage advancements in areas such as machine learning, blockchain, and hardware security to enhance the security of IoT environments.

Machine Learning for Anomaly Detection: Machine learning algorithms can be used to detect anomalies in IoT network traffic and behavior, which may indicate a security threat. By analyzing patterns in data generated by IoT devices, machine learning models can identify deviations from normal behavior and trigger alerts for further investigation. This approach can help IoT networks detect and respond to security threats in real-time, improving overall security posture.

Blockchain for Secure Data Exchange: Blockchain technology offers a decentralized and tamper-resistant platform for secure data exchange in IoT networks. By leveraging blockchain's cryptographic features and distributed ledger, IoT devices can securely record and verify transactions without the need for a central authority. This enhances data integrity and confidentiality, making it difficult for attackers to manipulate or intercept data exchanged between IoT devices.

Hardware-based Security Solutions: Hardware-based security solutions, such as secure elements and trusted platform modules (TPM), provide a hardware-based root of trust for IoT devices. These hardware components store cryptographic keys and perform security-critical operations, such as encryption and authentication, in a secure environment. By offloading security functions to dedicated hardware, IoT devices can improve their resistance to attacks such as key extraction and tampering.

These novel methods and technologies demonstrate the potential to significantly enhance the security of IoT networks. By integrating these approaches into existing security frameworks, IoT stakeholders can strengthen their defenses against a wide range of cyber threats and ensure the continued growth and adoption of IoT technologies.

V. Case Studies

Examining real-world examples of IoT security frameworks and incidents can provide valuable insights into the effectiveness of existing security measures and the potential impact of security breaches.

Security Frameworks for IoT: Several organizations and standards bodies have developed security frameworks specifically tailored to the unique challenges of IoT environments. For example, the IoT Security Foundation (IoTSF) has published guidelines and best practices for securing IoT devices and networks. These frameworks emphasize the importance of implementing security measures at every stage of the IoT lifecycle, from device design and manufacturing to deployment and maintenance.

Real-world Examples of IoT Security Breaches: Despite efforts to improve security, IoT devices remain vulnerable to cyber attacks. One notable example is the Mirai botnet attack in 2016, which exploited insecure IoT devices to launch large-scale distributed denial-of-service

(DDoS) attacks. This incident highlighted the importance of securing IoT devices against unauthorized access and the need for proactive security measures to prevent similar attacks in the future.

By studying these case studies, IoT stakeholders can gain a better understanding of the security challenges facing IoT networks and the importance of implementing robust security measures to protect against potential threats.

VI. Future Directions

The field of IoT security is rapidly evolving, driven by ongoing research and development efforts to address emerging threats and challenges. Several key areas are shaping the future of IoT security, including the adoption of emerging technologies, the establishment of standards and regulations, and the collaboration between industry stakeholders.

Emerging Technologies for IoT Security: Emerging technologies such as artificial intelligence (AI), quantum cryptography, and edge computing are poised to play a significant role in enhancing IoT security. AI-powered security solutions can improve threat detection and response capabilities, while quantum cryptography offers the potential for ultra-secure communication channels. Edge computing enables security functions to be performed closer to IoT devices, reducing latency and improving overall security.

Standards and Regulations: The development of standards and regulations for IoT security is essential to ensure a consistent and effective approach to security across IoT devices and networks. Organizations such as the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) are actively working to develop guidelines and frameworks for IoT security. Compliance with these standards can help mitigate security risks and enhance the overall security posture of IoT ecosystems.

Industry Collaboration: Collaboration between industry stakeholders, including device manufacturers, service providers, and regulators, is crucial for addressing IoT security challenges. By sharing best practices, threat intelligence, and lessons learned, stakeholders can collectively improve the security of IoT networks and devices. Initiatives such as the

Cybersecurity Tech Accord and the Open Web Application Security Project (OWASP) provide platforms for industry collaboration on IoT security.

By focusing on these future directions, the IoT industry can continue to innovate and advance IoT security, ensuring the continued growth and success of IoT technologies across various domains.

VII. Conclusion

In conclusion, securing IoT networks is critical to protect against the increasing threats posed by cyber attacks. The challenges inherent in IoT security, such as resource constraints, device heterogeneity, and scalability issues, require innovative approaches and technologies to enhance security protocols and defenses. While existing security mechanisms provide a foundational level of security, novel methods such as machine learning for anomaly detection, blockchain for secure data exchange, and hardware-based security solutions offer promising avenues for improving IoT security.

Furthermore, case studies of IoT security frameworks and incidents underscore the importance of implementing robust security measures and adhering to best practices. Looking ahead, the adoption of emerging technologies, the establishment of standards and regulations, and industry collaboration will play a crucial role in shaping the future of IoT security.

By addressing these challenges and embracing these opportunities, the IoT industry can build a safer and more secure IoT ecosystem, enabling the continued growth and adoption of IoT technologies across various domains.

References

Pargaonkar, Shravan. "A Review of Software Quality Models: A Comprehensive Analysis." *Journal of Science & Technology* 1.1 (2020): 40-53.

Ding, Liang, et al. "Understanding and improving lexical choice in non-autoregressive translation." *arXiv preprint arXiv:2012.14583* (2020).

Vyas, Bhuman. "Java in Action: AI for Fraud Detection and Prevention." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* (2023): 58-69.

Reddy, Surendranadha Reddy Byrapu, and Surendranadha Reddy. "Large Scale Data Influences Based on Financial Landscape Using Big Data." *Tuijin Jishu/Journal of Propulsion Technology* 44.4 (2023): 3862-3870.

Singh, Amarjeet, et al. "Improving Business deliveries using Continuous Integration and Continuous Delivery using Jenkins and an Advanced Version control system for Microservices-based system." *2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)*. IEEE, 2022.

Ding, Liang, Di Wu, and Dacheng Tao. "Improving neural machine translation by bidirectional training." *arXiv preprint arXiv:2109.07780* (2021).

Raparthi, Mohan, Sarath Babu Dodda, and SriHari Maruthi. "Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks." *European Economic Letters (EEL)* 10.1 (2020).

Pargaonkar, Shravan. "Bridging the Gap: Methodological Insights from Cognitive Science for Enhanced Requirement Gathering." *Journal of Science & Technology* 1.1 (2020): 61-66.

Reddy, S. R. B., & Reddy, S. (2023). Large Scale Data Influences Based on Financial Landscape Using Big Data. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(4), 3862-3870.

Vyas, Bhuman. "Security Challenges and Solutions in Java Application Development." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 12.2 (2023): 268-275.

Raparthi, Mohan, Sarath Babu Dodda, and Srihari Maruthi. "AI-Enhanced Imaging Analytics for Precision Diagnostics in Cardiovascular Health." *European Economic Letters (EEL)* 11.1 (2021).

Ding, Liang, Longyue Wang, and Dacheng Tao. "Self-attention with cross-lingual position representation." *arXiv preprint arXiv:2004.13310* (2020).

Pargaonkar, Shravan. "Future Directions and Concluding Remarks Navigating the Horizon of Software Quality Engineering." *Journal of Science & Technology* 1.1 (2020): 67-81.

Vyas, Bhuman. "Ensuring Data Quality and Consistency in AI Systems through Kafka-Based Data Governance." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 10.1 (2021): 59-62.

Raparthi, Mohan, et al. "AI-Driven Metabolmics for Precision Nutrition: Tailoring Dietary Recommendations based on Individual Health Profiles." *European Economic Letters (EEL)* 12.2 (2022): 172-179.

Pargaonkar, Shravan. "Quality and Metrics in Software Quality Engineering." *Journal of Science & Technology* 2.1 (2021): 62-69.

Ding, Liang, et al. "Rejuvenating low-frequency words: Making the most of parallel data in non-autoregressive translation." *arXiv preprint arXiv:2106.00903* (2021).

Reddy, Byrapu, and Surendranadha Reddy. "Demonstrating The Payroll Reviews Based On Data Visualization For Financial Services." *Tuijin Jishu/Journal of Propulsion Technology* 44.4 (2023): 3886-3893.

Vyas, Bhuman. "Explainable AI: Assessing Methods to Make AI Systems More Transparent and Interpretable." *International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal* 10.1 (2023): 236-242.

Singh, Amarjeet, et al. "Event Driven Architecture for Message Streaming data driven Microservices systems residing in distributed version control system." *2022 International Conference on Innovations in Science and Technology for Sustainable Development (ICISTSD)*. IEEE, 2022.

Pargaonkar, Shravan. "The Crucial Role of Inspection in Software Quality Assurance." *Journal of Science & Technology* 2.1 (2021): 70-77.

Reddy, B., & Reddy, S. (2023). Demonstrating The Payroll Reviews Based On Data Visualization For Financial Services. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(4), 3886-3893.

Ding, Liang, et al. "Context-aware cross-attention for non-autoregressive translation." *arXiv preprint arXiv:2011.00770* (2020).

Vyas, Bhuman. "Optimizing Data Ingestion and Streaming for AI Workloads: A Kafka-Centric Approach." *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068* 1.1 (2022): 66-70.

Rajendran, Rajashree Manjulalayam. "Scalability and Distributed Computing in NET for Large-Scale AI Workloads." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 10.2 (2021): 136-141.

Pargaonkar, Shravan. "Unveiling the Future: Cybernetic Dynamics in Quality Assurance and Testing for Software Development." *Journal of Science & Technology* 2.1 (2021): 78-84.

Vyas, Bhuman. "Java-Powered AI: Implementing Intelligent Systems with Code." *Journal of Science & Technology* 4.6 (2023): 1-12.

Nalluri, Mounika, et al. "Investigate The Use Of Robotic Process Automation (RPA) To Streamline Administrative Tasks In Healthcare, Such As Billing, Appointment Scheduling, And Claims Processing." *Tuijin Jishu/Journal of Propulsion Technology* 44.5 (2023): 2458-2468.

Vyas, Bhuman. "Ethical Implications of Generative AI in Art and the Media." *International Journal for Multidisciplinary Research (IJFMR), E-ISSN*: 2582-2160.

Ding, Liang, et al. "Redistributing low-frequency words: Making the most of monolingual data in non-autoregressive translation." *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. 2022.

Rajendran, Rajashree Manjulalayam. "Exploring the Impact of ML NET (http://ml. net/) on Healthcare Predictive Analytics and Patient Care." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 11.1 (2022): 292-297.

Nalluri, M., Reddy, S. R. B., Rongali, A. S., & Polireddi, N. S. A. (2023). Investigate The Use Of Robotic Process Automation (RPA) To Streamline Administrative Tasks In Healthcare, Such As Billing, Appointment Scheduling, And Claims Processing. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(5), 2458-2468.

Pargaonkar, Shravan. "Unveiling the Challenges, A Comprehensive Review of Common Hurdles in Maintaining Software Quality." *Journal of Science & Technology* 2.1 (2021): 85-94.

Nalluri, Mounika, and Surendranadha Reddy Byrapu Reddy. "babu Mupparaju, C., & Polireddi, NSA (2023). The Role, Application And Critical Issues Of Artificial Intelligence In Digital Marketing." *Tuijin Jishu/Journal of Propulsion Technology* 44.5: 2446-2457.

Pargaonkar, S. (2020). A Review of Software Quality Models: A Comprehensive Analysis. *Journal of Science & Technology*, *1*(1), 40-53.

Nalluri, M., & Reddy, S. R. B. babu Mupparaju, C., & Polireddi, NSA (2023). The Role, Application And Critical Issues Of Artificial Intelligence In Digital Marketing. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(5), 2446-2457.

Singh, A., Singh, V., Aggarwal, A., & Aggarwal, S. (2022, November). Improving Business deliveries using Continuous Integration and Continuous Delivery using Jenkins and an Advanced Version control system for Microservices-based system. In *2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)* (pp. 1-4). IEEE.

Vyas, Bhuman, and Rajashree Manjulalayam Rajendran. "Generative Adversarial Networks for Anomaly Detection in Medical Images." *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068* 2.4 (2023): 52-58.

Raparthi, M., Dodda, S. B., & Maruthi, S. (2020). Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks. *European Economic Letters (EEL)*, *10*(1).

Pargaonkar, S. (2020). Bridging the Gap: Methodological Insights from Cognitive Science for Enhanced Requirement Gathering. *Journal of Science & Technology*, *1*(1), 61-66.

Nalluri, Mounika, et al. "Explore The Application Of Machine Learning Algorithms To Analyze Genetic And Clinical Data To Tailor Treatment Plans For Individual Patients." *Tuijin Jishu/Journal of Propulsion Technology* 44.5 (2023): 2505-2513.

Raparthi, M., Dodda, S. B., & Maruthi, S. (2021). AI-Enhanced Imaging Analytics for Precision Diagnostics in Cardiovascular Health. *European Economic Letters (EEL)*, *11*(1).

Vyas, B. (2021). Ensuring Data Quality and Consistency in AI Systems through Kafka-Based Data Governance. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *10*(1), 59-62.

Rajendran, R. M. (2021). Scalability and Distributed Computing in NET for Large-Scale AI Workloads. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *10*(2), 136-141.

Nalluri, M., Reddy, S. R. B., Pulimamidi, R., & Buddha, G. P. (2023). Explore The Application Of Machine Learning Algorithms To Analyze Genetic And Clinical Data To Tailor Treatment Plans For Individual Patients. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(5), 2505-2513.

Singh, A., Singh, V., Aggarwal, A., & Aggarwal, S. (2022, August). Event Driven Architecture for Message Streaming data driven Microservices systems residing in distributed version control system. In *2022 International Conference on Innovations in Science and Technology for Sustainable Development (ICISTSD)* (pp. 308-312). IEEE.

Pargaonkar, S. (2020). Future Directions and Concluding Remarks Navigating the Horizon of Software Quality Engineering. *Journal of Science & Technology*, *1*(1), 67-81.

Vyas, B. (2022). Optimizing Data Ingestion and Streaming for AI Workloads: A Kafka-Centric Approach. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *1*(1), 66-70.

Pargaonkar, S. (2021). Quality and Metrics in Software Quality Engineering. *Journal of Science & Technology*, *2*(1), 62-69.

Byrapu, Surendranadha Reddy. "Big Data Analysis in Finance Management." *JOURNAL OF ALGEBRAIC STATISTICS* 14.1 (2023): 142-149.

Rajendran, Rajashree Manjulalayam. "Code-driven Cognitive Enhancement: Customization and Extension of Azure Cognitive Services in. NET." *Journal of Science & Technology* 4.6 (2023): 45-54.

Vyas, B. Ethical Implications of Generative AI in Art and the Media. *International Journal for Multidisciplinary Research (IJFMR), E-ISSN*, 2582-2160.

Rajendran, R. M. (2022). Exploring the Impact of ML NET (http://ml. net/) on Healthcare Predictive Analytics and Patient Care. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *11*(1), 292-297.

Pargaonkar, S. (2021). The Crucial Role of Inspection in Software Quality Assurance. *Journal of Science & Technology*, *2*(1), 70-77.

Raparthi, Mohan. "Predictive Maintenance in Manufacturing: Deep Learning for Fault Detection in Mechanical Systems." *Dandao Xuebao/Journal of Ballistics* 35: 59-66.

Byrapu, S. R. (2023). Big Data Analysis in Finance Management. *JOURNAL OF ALGEBRAIC STATISTICS*, *14*(1), 142-149.

Pargaonkar, S. (2021). Unveiling the Future: Cybernetic Dynamics in Quality Assurance and Testing for Software Development. *Journal of Science & Technology*, *2*(1), 78-84.

Rajendran, Rajashree Manjulalayam. "Importance Of Using Generative AI In Education: Dawn of a New Era." *Journal of Science & Technology* 4.6 (2023): 35-44.

Raparthi, Mohan. "Biomedical Text Mining for Drug Discovery Using Natural Language Processing and Deep Learning." *Dandao Xuebao/Journal of Ballistics* 35.

Raparthi, M., Maruthi, S., Dodda, S. B., & Reddy, S. R. B. (2022). AI-Driven Metabolmics for Precision Nutrition: Tailoring Dietary Recommendations based on Individual Health Profiles. *European Economic Letters (EEL)*, *12*(2), 172-179.

Pargaonkar, S. (2021). Unveiling the Challenges, A Comprehensive Review of Common Hurdles in Maintaining Software Quality. *Journal of Science & Technology*, *2*(1), 85-94.

Raparthy, Mohan, and Babu Dodda. "Predictive Maintenance in IoT Devices Using Time Series Analysis and Deep Learning." *Dandao Xuebao/Journal of Ballistics* 35: 01-10.

Alami, Rachid, Hamzah Elrehail, and Amro Alzghoul. "Reducing cognitive dissonance in health care: Design of a new Positive psychology intervention tool to regulate professional stress among nurses." *2022 International Conference on Cyber Resilience (ICCR)*. IEEE, 2022.

Alami, Rachid. "Paradoxes and cultural challenges: case of Moroccan manager returnees and comparison with Chinese returnees." *International Journal of Management Development* 1.3 (2016): 215-228.

Alami, Rachid. "Innovation challenges: Paradoxes and opportunities in China." *The ISM Journal of International Business* 1.1 (2010): 1G.

Aroussi, Rachid Alami, et al. "Women Leadership during Crisis: How the COVID-19 Pandemic Revealed Leadership Effectiveness of Women Leaders in the UAE." *Migration Letters* 21.3 (2024): 100-120.

Bodimani, Meghasai. "AI and Software Engineering: Rapid Process Improvement through Advanced Techniques." *Journal of Science & Technology* 2.1 (2021): 95-119.

Bodimani, Meghasai. "Assessing The Impact of Transparent AI Systems in Enhancing User Trust and Privacy." *Journal of Science & Technology* 5.1 (2024): 50-67.