A Comprehensive Review of Security and Privacy Issues in Resource-Constrained IoT Based on Nanotechnology Systems

Dr. Anupa Sinha[1], Yalakala Dinesh Kumar[2]

[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.

Throughout the history of humanity, multiple tools have been developed and utilized to improve the quality of life, thanks to groundbreaking innovations that determine the future of humanity. These technologies have shaped the current state and are integral to essential aspects of human existence, including agriculture, medical care, and transportation. The Internet of Things (IoT) is a system that has profoundly transformed several aspects of the lives. It emerged in the early 21st century alongside the progress of Internet and Information Communication (ICT) Technology. The IoT has gradually developed and opened the possibility for the Internet of Nano-Things (IoNT), which involves utilizing nano-scale small IoT devices. The IoNT is an emerging technology gaining recognition, particularly in academic and research circles. Utilizing the IoNT inevitably incurs expenses due to its connection to the Internet and the inherent susceptibility of IoNT devices, which creates opportunities for hackers to exploit security and privacy. The research has been encouraged to study in the IoNT domain due to the existing gap in knowledge. The research aims to synthesize information on architectural features in the IoNT environment and address the security and privacy problems associated with the IoNT. The research examines the IoNT ecosystem and its associated security and privacy concerns. This analysis serves as a valuable resource for upcoming studies in this field.

Keywords: Security, Privacy, Internet of Things, Nanotechnology.

1. Introduction

The exponential growth and high need for Information and Communication Technologies (ICT) in the early 21st century have significantly impacted various sectors, including

manufacturing, transportation, interactions, medical care, and agriculture, enabling them to achieve their maximum capabilities [1]. This has resulted in the widespread adoption of technological advances such as the Internet of Things (IoT) [2], Artificial Intelligence (AI) [10], and cloud computing. This technology enables vital players to connect all digital devices in these sectors to the internet, enabling quick information sharing and integrating with advanced technologies like AI. This integration allows for real-time analysis and governance, making these sectors more intelligent and widely accessible.

The IoT has fully transformed how individuals utilize the Internet and device-to-device (D2D) communication. This refers to how gadgets, detectors, and objects communicate and share information. It has opened up possibilities for the IoT on a minuscule scale, known as the Internet of Nano-Things (IoNT) [4]. The IoT and the IoNT can be consolidated into a concept known as the Internet of Everything (IoE) [5].

The IoNT has already surpassed its adolescent stage and is ready to make a significant impact worldwide. IoNT is an emerging technology that has recently gained considerable attention. IoNT implies the integration of nanoscale devices into pre-existing networks. The IoNT comprises connected networks of nanoscale gadgets capable of communication and data exchange among themselves and larger systems [6]. These technologies can transform various industries, including agriculture and healthcare [12].

The utilization of nanotechnologies inside an IoT system is highly diverse and contingent upon the specific circumstances. Smart manufacturing companies utilize IoT gadgets to monitor various environmental factors such as humidity, water temperatures, quantity, and air pollution. Contemporary vehicles with equally compact sensors can make precise forecasts regarding proximity, climatic conditions, and positional data. This capability ensures the safety and effectiveness of driver assistance technologies [8]. In smart cities, IoNT systems already in place are liable for monitoring harmful gasses or particulate levels. Strategically positioned devices would be installed in multiple areas across the city to track pollution levels, ensuring the well-being and safety of the population [9].

An inherent security vulnerability of the IoNT is the possibility for malicious individuals to obtain confidential information being communicated by these interconnected devices illicitly [11]. Due to their compact size and widespread deployment, it might be challenging to identify whether these gadgets have been infiltrated. The information these gadgets convey, such as medical records or banking information, is sensitive. If unauthorized parties accessed this material, it would result in significant repercussions for the individuals concerned. IoNT poses a risk of Denial-Of-Service (DoS) assaults [7]. These assaults occur when a malevolent actor inundates a device or network with a large amount of traffic, causing it to become incapable of functioning correctly. Given that the IoNT comprises numerous connected gadgets, a DoS assault on a single item could have a widespread impact on the entire network. The potential consequences could be significant, mainly when the IoNT is utilized for critical facilities or rescue services.

IoNT gives rise to problems around privacy. The widespread use of these devices implies that individuals can be continuously observed and traced, potentially enabling firms or governments to collect vast quantities of personal information. This data can be utilized for focused advertising or be traded to external entities without the individual's awareness or

agreement, compromising their privacy [3].

2. Architecture of IoNT

The IoNT structure is characterized by a diverse array of technologies and procedures to enhance interaction and exchange of information at the nanoscale, making it more intricate than the IoNT. The essential elements of the IoNT architecture consist of nanosensors and actuation. The core components of the IoNT can detect and quantify a wide range of physical, chemical, and biological factors. They can execute actions according to the data collected.

- Communication

The IoNT utilizes several communication protocols, including wireless systems like Radio-Frequency Identification (RFID), Bluetooth connectivity, near-field interactions, and wired innovations, such as nanowires and nanotubes, to facilitate interaction among nanotechnology objects. These methods enable small gadgets to communicate by sending and receiving data over nano distances.

- Processing and data storage

Specialized data processing and storage techniques are necessary to handle and retain the vast data produced by the IoNT. These developments encompass nanoscale storage devices, such as memory devices that utilize nanocapacitors, and nano computation devices, including quantum computing gadgets or cellular computing systems.

- Network system

The IoNT depends on a network architecture of routers, switches, and other networking equipment to facilitate interaction among nano gadgets and other gadgets connected to the Internet. This architecture consists of conventional networking methods, and technologies developed explicitly for the nanoscale. After summarizing the essential elements in the framework of the IoNT, the research examined the structure of an individual nanomachine, which serves as the basis for more intricate IoNT solutions. A nanomachine comprises the following elements:

- The control unit oversees and manages all other elements of the nanomachine and is tasked with gathering environmental information.
- The communication component is tasked with transmitting and receiving data at the nanoscale.
- The reproductive unit utilizes outside elements to fabricate each constituent of the nanomachine and subsequently builds them to generate the final nanomachine.

3. Challenges of IoNT systems

3.1 Privacy and Security

Users of the IoNT architecture should be informed about the individuals accessing their data and how their data will be employed [13]. This is because nanodevices collect large amounts

of confidential data, which necessitates careful consideration of protection and security measures. Storing the collected data in a secure location with robust encryption and state-of-the-art network security measures is imperative. Whenever left vulnerable, attackers can illicitly access this private data. IoNT engineers must carefully consider these difficulties before extensively producing and using IoNT gadgets.

3.2 Compatibility

When creating clinical nanosensors, researchers must guarantee that these nanosensors do not have any unintended effects on a patient's health. Discovering such substances will necessitate extensive testing, which can be time-consuming and prone to errors.

3.3 Invasion vectors In IoNT

An invasion vector refers to the method via which an attacker gains unauthorized access to a computer or network to deliver a payload or cause a negative effect. An invasion vector refers to gaining access to a computer or network to deliver a payload or malicious outcome. Exploiting assault vectors can be used to get unauthorized access to important details, including personally identifiable information and other confidential data, resulting in a data breach. It seeks to exploit the vulnerabilities in a device or a corporation. There are several potential ways in which the IoNT architecture can be compromised, and it is essential to address these vulnerabilities by implementing appropriate security measures.

- Internet Exposure

Any device that connects to the Internet and accepts incoming communication is inherently susceptible to many types of assaults. Nanodevices, due to their limited computational capabilities and memory and the absence of built-in security features, are vulnerable to diverse attacks originating from different locations on the Internet.

- Lack of Encryption

Security is often an afterthought in the development process of IoNT devices. Encryption is uncommon in most nano gadgets due to their small size and limited computational capabilities. The absence of encryption for information transmitted between nano gadgets, whether on the gadgets themselves or within nano organizations, leads to significant security concerns, particularly when nano gadgets become integrated into human bodies. Installing cryptography, such as crypto-feasible co-processors, is necessary to encrypt and authenticate nano gadgets. Acquiring information from nano gadgets is crucial for any strategy.

- DoS

DoS is a type of cyber assault in which a malicious actor intentionally disrupts a computer's or other device's normal functioning, rendering it inaccessible to its intended users. In this scenario, the attacker attempts to manipulate the availability of an organization, which can be challenging to guarantee, as assailants possess sufficient power to radio transmissions or flood the communication channel with excessive particles that disrupt everyday communication.

3.4 Security in nano-things

The IoNT is vulnerable to various types of attacks, including both physical and remote methods. Assaults can occur to obtain confidential information by stealing sensors, disrupting programs operated by computers, or altering the communication links inside nano-networks. These devices have their control and monitoring mechanisms digitized and connected to the Internet, which gives rise to many security and safety concerns [9]. The primary challenges associated with the growth of the IoNT market are related to the security of data transmitted over the Internet. The IoNT is vulnerable to various attacks, both physical and through wireless technologies, because of its lack of constant vigilance.

Assaults can occur to obtain confidential data via stealing sensors, infiltrating apps operated by computers, or manipulating communication links in nanonetworks. The security targets encompass the principles of confidentiality, integrity, and availability. When integrated with IoNT, nano-specific gadgets face security challenges often encountered by regular sensor networks. The accessibility of entering center points and the proliferation of mobile devices have significantly expanded the potential attack vectors for assailants. Utilizing these organizations for social events involves highly confidential data ranging from location to physiological information, rendering these organizations a prime target for malicious individuals. Implementing new security and protection protocols to safeguard sensitive data collected by nanosensors is necessary.

4. Conclusion and findings

The swift proliferation of nanotechnology and its fusion with the IoT has opened up opportunities for the IoNT, which is experiencing exponential growth in several fields, such as smart cities, smart farming, the military, medical care, and more. Due to its small size and advantages compared to the IoT, the IoNT is increasingly becoming a crucial aspect of everyday existence. While technology provides numerous benefits, utilizing IoNT technology is expensive due to its reliance on Internet connectivity, susceptibility to inherent weaknesses, and small size. These drawbacks exceed the majority of the advantages and provide substantial concerns regarding security and privacy. To address these points, the research has comprehensively analyzed the security and privacy concerns associated with the IoNT. The research presents a comprehensive analysis of the IoNT, focusing on the current status of research, the architectural framework, diverse applications, advantages, and security and privacy aspects. The research addressed the obstacles related to security and confidentiality that impede the effective implementation of security and privacy measures in the IoNT. The research classified security and privacy threats according to their attack methods and presented solutions to counteract them and potential areas for future research. To effectively safeguard the IoNT, it is necessary to employ stringent security and privacy measures at the micro-scale level despite the inherent security vulnerability at the nanoscale.

References

1. Ahmed, Z., & Le, H. P. (2021). Linking Information Communication Technology, trade

globalization index, and CO2 emissions: evidence from advanced panel techniques. Environmental Science and Pollution Research, 28(7), 8770-8781.
2. Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). A review and state of the art of the Internet of Things (IoT). Archives of Computational Methods in Engineering, 1-19.
3. Dr.R. Mohandas, Dr.S. Veena, G. Kirubasri, I. Thusnavis Bella Mary, & Dr.R. Udayakumar. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data. Indian Journal of Information Sources and Services, 14(2), 17–23. https://doi.org/10.51983/ijiss-2024.14.2.03
4. Al-Turjman, F. (2020). A cognitive routing protocol for bio-inspired networking in the Internet of nano-things (IoNT). Mobile Networks and Applications, 25(5), 1929-1943.
5. Farias da Costa, V. C., Oliveira, L., & de Souza, J. (2021). Internet of Everything (IoE) taxonomies: A survey and a novel knowledge-based taxonomy. Sensors, 21(2), 568.
6. Udayakumar, R., Anuradha, M., Gajmal, Y. M., & Elankavi, R. (2023). Anomaly detection for internet of things security attacks based on recent optimal federated deep learning model. Journal of Internet Services and Information Security, 13(3), 104-121.
7. Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in the cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 39, 100332.
8. Al-Turjman, F. (2020). Intelligence and security in big 5G-oriented IoNT: An overview. Future generation computer systems, 102, 357-368.
9. Skarmeta, A.F., Cano, M.V.M., & Iera, A. (2015). Guest Editorial: Smart Things, Big Data Technology and Ubiquitous Computing solutions for the future Internet of Things. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6(1), 1-3.
10. George, Reny, et al. "Some existential fixed point results in metric spaces equipped with a Graph and it's application." Results in Nonlinear Analysis 7.1 (2024): 122-141.
11. Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224.
12. Rai, S., Patnaik, S., Rupani, A., Knechtel, J., Sinanoglu, O., & Kumar, A. (2020). Security promises and vulnerabilities in emerging reconfigurable nanotechnology-based circuits. IEEE Transactions on Emerging Topics in Computing, 10(2), 763-778.
13. Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.
14. Zafar, S., Nazir, M., Bakhshi, T., Khattak, H. A., Khan, S., Bilal, M., ... & Sabah, A. (2021). A systematic review of bio-cyber interface technologies and security issues for the internet of bio-nano things. IEEE Access, 9, 93529-93566.