RESEARCH ARTICLE | MARCH 29 2023

Security in internet of nano things (IoNT): Challenges and suggested solutions

Hayder A. Naser; Mothefer M. Jahefer; Hadi R. Ali; ... et. al

AIP Conference Proceedings 2591, 030026 (2023)
https://doi.org/10.1063/5.0119645

Security in Internet of Nano Things (IoNT): Challenges and Suggested Solutions

Hayder A. Naser [a)], Mothefer M. Jahefer [b)], Hadi R. Ali [c)] and Huda H. Ali [d)]

Department of Computer Techniques Engineering, Imam Alkadhum College (IKC), Baghdad, Iraq.

[a)] *hayder.a.naser@gmail.com*
[b)] *mothefer82.82@gmail.com*
[c)] *itech.hadi@gmail.com*
[d)] *Corresponding author: huda.hamdan33@gmail.com*

Abstract. The advancement in nanotechnology has affected different fields of technologies. One of these fields is the IoT, which represents a new version of the internet, and so that a new descendent of IoT has emerged and named the Internet of Nano Things (IoNT). Today, IoNT is utilized in many aspects of life, such as smart cities, industries, infrastructure maintenance and monitoring, healthcare services and others. More, IoNT applications could be a must solution in certain cases such as in the healthcare field. However, to apply IoNT systems in real life, some challenges have to be considered such as communication methods, security, and privacy issues. In that regard, this article aims to discuss the security issues in IoNT and suggest solutions for them in light of some recently published studies. In addition, the main features of security in IoNT are discussed and the most challenging problems are identified**.** Eventually, since the IoNT technology is still considered in the starting steps, the research in this area could be helpful to other interested researchers.

Keywords: IoNT, Nano device, Security Challenges, Nano Communications, Suggested Solutions.

INTRODUCTION

Internet of Nano-Things (IoNT) is one of the IoT specific Applications developed to justified different domains of, communication [1]. IoNT describes a new field of communications deals with nano components with a super feature characterized this technique due to it range of work which investigates cost reduction [2]. This technique has interesting in the implementation of different states of applications such as social, health and telemedicine [3]. security problem is one of the most important issues resulting from this technology and related to the data that is handled and sent, because this data is subject to theft and threat and needs to be processed in a new framework that fits with this advanced technology. Despite the progress made in the field of health applications, other applications still need more studies [4].

In [5] the secure parameters of IoNT with a secure proposal have been presented. An overview study dealt with security threat states are designed by [6] conjugated with IoNT communication. In [7] some solutions are proposed to address the encryption problem at the molecular level by reducing the computational operations within the nanonetwork in radio physical layer security (PLS). The creation of a new state of safety in nano-networks to counter potential external attacks was studied and evaluated in [8]. A design was studied in the terahertz band channel, and the security problems it faces in terms of encryption and communication between the components of the system are identified by [9] with a discussion of security challenges in terms of authentication, privacy and data integrity. IoMNT has not been mentioned in the IoT categories [1]; representative studies encourage it to be considered within the IoNT. The author proposed in [10] A study on the foundations of security-based communications, which includes new ways to provide security in communication networks. The IoNT security mechanisms have been investigated by [11]. In this work, most of the security problems mentioned by researchers during the last few period (2015-2021) were investigated during the design of nanonets, and the proposed solutions to these contemporary challenges were studied

Al-Kadhum 2nd International Conference on Modern Applications of Information and Communication Technology
AIP Conf. Proc. 2591, 030026-1–030026-7; https://doi.org/10.1063/5.0119645
Published by AIP Publishing. 978-0-7354-4324-2/$30.00

in order to facilitate the task of researchers on these issues and provide support by providing these data in a way easy. The recommendations in this regard have also been studied.

ARCHITECTURE OF IONT SECURITY SYSTEM

IoNT is subdivided into: Internet of the Nano-Things Multimedia (IoMNT) and Internet of the Bio-Nano Things (IoBNT), the technique type corresponding each part are shown in Figure 1. IoMNT represents the general applications of nano materials utilizing the internet with nano electromagnetic communication (EM) technique, while IoBNT It only includes medical applications with molecular communication [12].

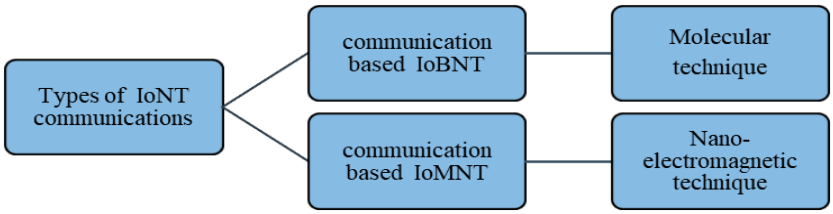

FIGURE 1. IoNT's Types of Communications.

Generally, the band used in IoNT is from 0.1THz to 10THz, which produces the advantage of super transmission with the huge amount of data. In molecular technology the coding is either as a core or as a type of transmitter molecule. Messenger molecules are used to store information through a medium, such as air or liquid. Which is limited by the short range due to the short wavelength of this technique, like correspondence in (Body Area Network) BANs. The main steps of IoNT communication are shown in Figure2 [13].

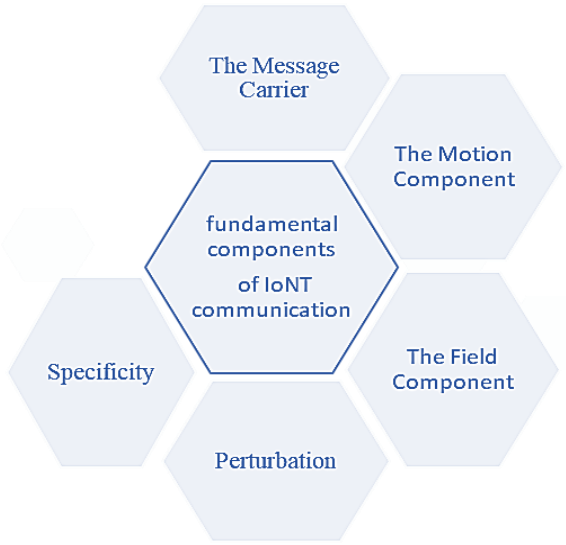

FIGURE 2. The main components of an IoNT network. Which include Message Carrier, Movement, Field, Turbulence, and Privacy.

The nano-network structure consists of a group of nano-devices that together constitute the basic structure of the nano-communication system, as shown in Figure 3, which describes this technology in the health field. It collects data from within the cells of the body, processes it, and then sends it to specialized receiving stations that take the necessary action and redirect it [14].

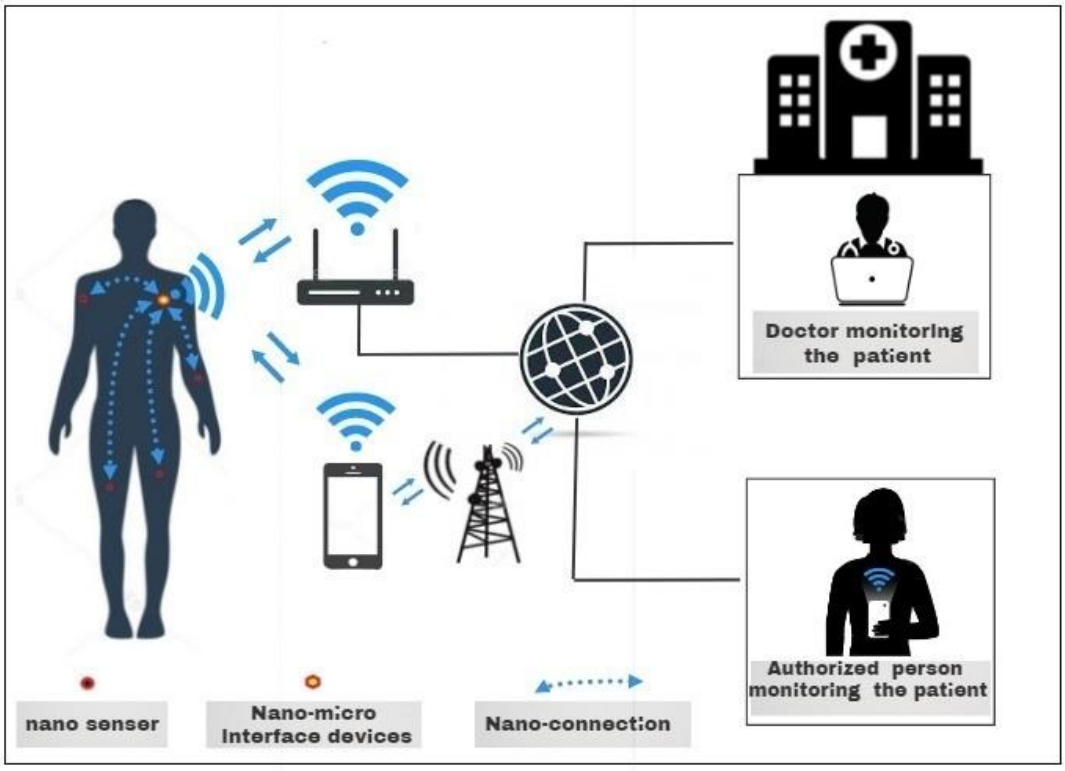

FIGURE 3. Typical Architecture and Common Components of IoNT.

In this technique, the problem can be identified within the delicate and difficult areas, and it can be treated by developing solutions to the problems facing this technology, such as including incoming messages, activation or deactivation commands, and the development of processing technology [15]. Several events can be encoded by the Nano sensors within the terahertz frequency region [16]. This technology is vulnerable to hacking, reprogramming, or network disruption as a result of weak security systems for IoT devices [17]. This requires more efforts to develop the IoNT network by increasing the processing and storage capabilities at reasonable costs, as well as developing models of antennas and RFID. The most important key points to achieve security within nanonets are illustrated in Figure 4. Table 1 shows the most important steps involved in the IoNT secure systems.

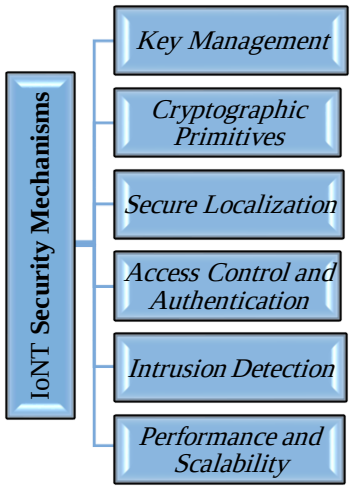

FIGURE 4. Security Mechanism Related to IoNT Techniques.

TABLE 1. Security specifications in IoNT network [18].

Authentication	Data Integrity	System Security	Internet Security
Identification	Encryption	Communication	Personal Health Records
Signature	Data Integrity Process	Processing	Secure Internet Services
Non-repudiation	Permanence	Storage	
		Permanence	

Table 1 shows the basic principles used at each stage of the IoNT to ensure its security. These standards contribute to addressing the problem of penetration of this technology during its various applications.

In order to verify the neighbor detection algorithms that determine the position and orientation between the nano-components Nano-machine manipulation must be investigated by exploiting the high direction of the antenna [8] [14]. While information routing can be implemented by defining a pulse-based communication system and programming the nano-nodes to be able to determine the dimensions between them [19].

CHALLENGES OF SECURITY IN IONT TECHNIQUE

As a result of the wide variety of capabilities of Nano-devices provided by IoNT technology in order to perform the task of collecting the required information. This leads to the emergence of a heterogeneity between these advanced devices and the appropriate software, which leads to a problem in data collection and the way to preserve it and other security challenges. The most famous types of security challenges in this technology can be summarized in figure 5.

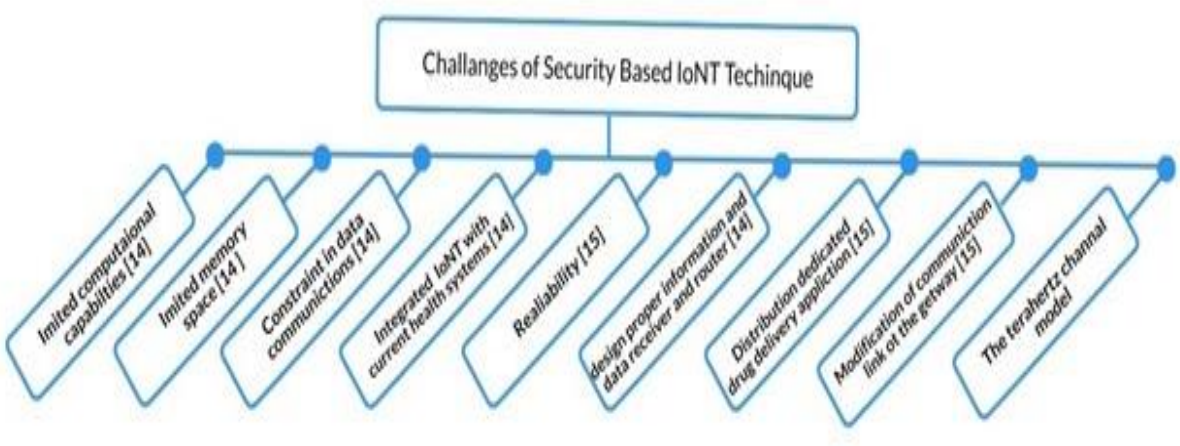

FIGURE 5. Security Challenges in IoNT

Among the most important reasons for the emergence of security challenges in IoNT technology that require solutions to them are as follows: [11]

1. Internet Exposure: The limited capabilities in the matter of data transmission and preservation is a security challenge in the Nano communication network.
2. Lack of Encryption*:* Because of the very small size of the Nano-devices, the encryption problem in these devices poses a challenge due to the difficulty of authentication between these devices and achieving high levels of security, which leads to hacking, and spying on private data [20].This challenge happens even at the level of molecular communication network [15]. One of the major challenges in IoNT technology is related to communication issues such as routing issues, processing capabilities, and power issues [3]. The poor use of

Nano-components is also responsible for achieving communication links inside the body with other components outside it [8]. Thus, the issue of using appropriate protocols to achieve an appropriate level of safety constitutes a priority in the field of application of this technology. The medical aspect is one of the most important applications of IoNT, and thus data security is considered a top priority in this field [21].

SOLUTIONS FOR SECURITY ISSUES IN IONT STUDIES

In this section, proposed solutions to some of the security challenges faced by IoNT technology will be studied. Among the most important areas that should be studied in the security aspect are:

New authentication mechanisms, ensure data integrity and user confidentiality. In Table 2, the most important proposed solutions to security challenges are summarized. These solutions are based on CIA security (Confidentiality, Integrity and Availability) in these new circumstances [22].

TABLE 2. Proposed Solutions for IoNT Security Problems.

IoNT Security Challenges	Solutions	Ref.
Cryptographic primitives in the scope of Body Area Networks (prevent the theft of private data)	Using the symmetric AES or the asymmetric RSA algorithms.	[15], [14]
Cryptographic primitives in the scope of In-Nano Communication	The biochemical cryptography	[24].
Key management (the ability of Creating and exchanging keys between the Body Area Network and the In-Body Nano Communication components	The gateway will have to part of a (possibly larger) PKI system.	[14].
improving the attainable security and securing the exchanged data	mm-Waves technique, called Silent Antenna Hopping (SAH)	[25]
satisfying security requirements	Security actions (activities) includes: (1) Scanning and Identification, (2) Authorization and Authentication Review, (3) Cluster Configuration and Deployment Control, and (4) Big Data Security Planning.	[6]
In molecular communication, an attacker could try to send arbitrary instructions into the In-Body Network.	Addressing schemes, real-time communication and low latency, communication reliability, application support	[8]
denial-of-service attacks that try to disrupt the availability of a system	An intrusion detection system can be used to handle this issue by detecting the attack and trigger the system to go into a fail-safe mode	[26].

RECOMMENDATIONS ABOUT IONT SECURITY

Developing components that contribute to improving Nano communication technology, such as designing nano microphones and headphones that integrate with this technology and contribute to positioning [12] [23]. Developing the basic components that contribute to the development of security and software capabilities of nanonetworks. Achieving the process of secure communication between the various Nano-devices in the IoNT system [7]. Development of new mechanisms for detecting intrusion at the nano level. As well as designing modern protocols related to security, with high performance and appropriate energy consumption [6]. Development of hardware technologies as well as encryption/decryption algorithms in IoNT, [5]. As well as deepening the understanding of the mechanisms of communication between the nano-components inside the body and their control [15]. Study of the factors affecting molecular contact such as absorption and its effects on the dispersion of contacts [6]. Improving Nanobots, Nano processors, Nano clocks, Nano-memory, improving IoNT tools, and reviewing new security and

protection systems regarding information collected by Nano sensors [17]. Develop solutions to the problem of eavesdropping by realizing physical layer security mechanisms [9].

CONCLUSIONS

It is not the opposite of the truth to say that research in IoNT technology is still in its beginning stages and its applications start to increase over time. The article has mentioned some challenges related to security in IoNT systems. On one hand, these conventional challenges in IoNT are explained such as key management, cryptographic primitives, access control and authentication, intrusion detection, and performance and scalability. On other hand, the most challenging features in IoNT networks are identified which are internet exposure and lack of encryption capability. Then, some proposed solutions to security problems in IoNT networks are outlined. These solutions can be classified into two types based on the challenge type. The first type of solutions is based on already established networks such as in IoT and WSN networks except that the solutions need to be adapted to work in the IoNT area, and the other solutions have to be originated exclusively. The reason for inventing new solutions is that IoNT networks have special properties such as the short distance of communication due to using the terahertz band, the sensitivity of its data as it may be related to persons such as in healthcare applications, and the nanoscale property of its devices. In addition, some recommendations are introduced according to recent articles research in IoNT. Eventually, the continuous research to tackle different challenges in IoNT and security is a major one of them will lead to open doors to emerging many applications.

REFERENCES

1. Ang, K. L. M., & Seng, J. K. P. Application specific internet of things (ASIoTs): Taxonomy, applications, use case and future directions. IEEE Access, 7, (2019), pp. 56577-56590.
2. Balghusoon, A. O., & Mahfoudh, S, Routing Protocols for Wireless Nanosensor Networks and Internet of Nano Things: A Comprehensive Survey. IEEE Access, 8, (2020), pp.200724-200748.
3. Cruz Alvarado, M. A., & Bazán, P, Understanding the Internet of Nano Things: overview, trends, and challenges. *E-Ciencias de la Información*, *9*(1), (2019), pp.152-182.
4. for Convergence in Technology (I2CT) IEEE, (pp. 371-375).
5. Pramanik, P. K. D., Solanki, A., Debnath, A., Nayyar, A., El-Sappagh, S., & Kwak, K. S. Advancing Modern Healthcare With Nanotechnology, Nanobiosensors, and Internet of Nano Things: Taxonomies, Applications, Architecture, and Challenges. IEEE Access, 8, (2020). , 65230-65266.
6. Al-Turjman, F. Intelligence and security in big 5G-oriented IoNT: An overview. Future Generation Computer Systems, 102, (2020) ,pp. 357-368.
7. Guo, W., Wei, Z., & Li, B. Secure Internet-of-Nano Things for Targeted Drug Delivery: Distance-based Molecular Cipher Keys. In 2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME) (2020, October), (pp. 1-6). IEEE.
8. Dressler, F., & Fischer, S. Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internet of Nano Things. Nano Communication Networks, 6(2), (2015),29-38.
9. Jornet, J. M., & Akyildiz, I. F. The internet of multimedia nano-things. Nano Communication Networks, 3(4), (2012),pp. 242-251.
10. Dressler, F., & Fischer, S. Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internetof Nano Things. Nano Communication Networks,2015; 6(2): pp.29–38.
11. Akhtar, N., & Perwej, Y. The internet of nano things (IoNT) existing state and future Prospects. *GSC Advanced Research and Reviews*, *5*(2), (2020), pp.131-150.
12. Balasubramaniam, S., Jornet, J. M., Pierobon, M., & Koucheryavy, Y. Guest editorial special issue on the internet of nano things. IEEE Internet of Things Journal, 3(1), (2016), pp.1-3.
13. Yang, K., Bi, D., Deng, Y., Zhang, R., Rahman, M., Ali, N. A., ... & Alomainy, A. A comprehensive survey on hybrid communication for internet of nano-things in context of body-centric communications. *arXiv preprint arXiv:* (2019),*1912.09424*.
14. Pramanik, P. K. D., Solanki, A., Debnath, A., Nayyar, A., El-Sappagh, S., & Kwak, K. S. Advancing Modern Healthcare With Nanotechnology, Nanobiosensors, and Internet of Nano Things: Taxonomies, Applications, Architecture, and Challenges. IEEE Access, 8, (2020). , pp.65230-65266.

15. Dressler, F., & Fischer, S. Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internet of Nano Things. Nano Communication Networks, 6(2), (2015), pp.29-38.
16. Panigrahi, T., & Hassan, M. Energy efficient event localization and classification for nano IoT. In 2018 IEEE Global Communications Conference (GLOBECOM) (2018, December), (pp. 1-6). IEEE.
17. Brijesh Khandelwal, Ashutosh choudhary, Ankit Mishra Realizing the Internet of Nano Things: A Review. International Journal of Emerging Trends in Engineering and Development Issue 8, Vol.3, (2018).
18. C. P. Waegemann. Confidentiality and Security for e-Health. Accessed: Dec. 10, 2018. [Online]. Available: https://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf
19. N. A. Ali and A. Ain, "Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges," in 2015 the First International Workshop on Advances in Body-Centric Wireless Communications and Networks and Their Applications, 2015, pp. 9–14.
20. O. M. E. and M. M., "The Future of Healthcare: Nanomedicine and Internet of Nano Things," Folia Medica - Fac. Med. Univ. Saraeviensis, 2015; vol. 50, no. 1: pp. 23–28.
21. Atlam, H. F., Walters, R. J., & Wills, G. BInternet of nano things: Security issues and applications. In Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing, (2018, August), pp. 71-77.
22. F. Dressler and S. Fischer, "Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internet of Nano Things," Nano Commun. Netw.; vol. 6, no. 2:pp. 29–38. GSC Advanced Research and Reviews, 2020, 05(02), pp.131–150.
23. Ali, N. A., & Abu-Elkheir, M. (2015, October). Internet of nano-things healthcare applications: Requirements, opportunities, and challenges. IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 (pp. 9-14).
24. F. Dressler, F. Kargl, Towards security in nano-communication: challenges and opportunities, Nano Commun. Netw. 3 (3) (2012) 151–160. http://dx.doi.org/10.1016/j.nancom.2012.08.001. Elsevier.
25. N.N. Alotaibi, K.A. Hamdi, Silent antenna hopping transmission technique for secure millimeter-wave wireless communication, in: 2015 IEEE Glob. Commun. Conf. (GLOBECOM), 2015, pp. 1–6.
26. M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks",IEEE 27th Conf. Comput. Commun.,2008; pp. 1238– 1246.