Internet of Nano Things: Security Issues and Applications

Hany F. Atlam
Electronic and Computer Science Dept., University of Southampton, Southampton, SO17 1BJ, UK
hfa1g15@soton.ac.uk

Robert J. Walters
Electronic and Computer Science Dept., University of Southampton, Southampton, SO17 1BJ, UK
rjw5@soton.ac.uk

Gary B. Wills
Electronic and Computer Science Dept., University of Southampton, Southampton, SO17 1BJ, UK
gbw@soton.ac.uk

ABSTRACT
Nanotechnology provides new solutions for numerous applications that have a significant effect on almost every aspect of our community including health monitoring, smart cities, military, agriculture, and industry. The interconnection of nanoscale devices with existing communication networks over the Internet defines a novel networking paradigm called the Internet of Nano-Things (IoNT). The IoNT involves a large number of nanosensors that used to provide more precise and detailed information about a particular object to enable a better understanding of object behaviour. In this paper, we investigate the challenges and opportunities of the IoNT system in various applications. An overview of the IoNT is first introduced. This is followed by a discussion of the network architecture of the IoNT and various applications that benefit from integrating IoT with nanotechnology. In the end, since security is considered to be one of the main issues of the IoNT system, we provide an in-depth discussion on security goals, attack vectors and security challenges of the IoNT system.

CCS Concepts
• **Security and privacy → Distributed systems security**

Keywords
Internet of Things; Nanotechnology; Security Challenges; Internet of Nano Things; IoNT applications; IoNT security.

1. INTRODUCTION
The popularity of the Internet of Things (IoT) is increasing every day, especially with existing and modern wireless telecommunications techniques. The IoT has the capability to connect and communicate all objects around us over the Internet using either wired or wireless networks [1]. There is no doubt that the IoT has changed the use of the Internet and Machine-to-Machine (M2M) communication in such a way to enable devices, sensors, and objects to communicate with one another and exchange their information to create new applications and services that used to improve human life's [2].

The IoT concept was first introduced by Kevin Ashton in 1999 [3]. Due to the rapid development in mobile communication, Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), and Cloud computing, communications among IoT devices has become easier and different objects are able to communicate and cooperate with each other. The IoT system involves a vast diversity of devices such as smartphones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices which generate a large scale network of heterogeneous devices [4].

The IoT has a critical effect on numerous aspects of everyone's life such as healthcare, agriculture, industry, smart cities, smart appliances, etc [5].

Nanotechnology has enabled better and efficient opportunities for numerous applications including health monitoring, industry, agriculture, smart cities, military, etc. It has resulted in the development of nanomachines, which are very small elements encompassing of organized set of molecules carrying out predetermined operations. Nanotechnology allows nanodevices to collect, create, compute, process and transmit data at nanoscale dimension. The interconnection of nanosensors and nanodevices with existing classical communication networks with the high-speed Internet has led to the evolution of what is called the Internet of Nano Things (IoNT) [2].

IoNT is the interconnection of nanoscale objects with the existing telecommunication networks. It enables new dimensions for the IoT by embedding nanosensors inside the objects to enable them to communicate and interact together through nanonetworks via the Internet [6]. In addition, IoNT explains how the Internet will evolve as nanosensors, which are in billions, will be connected and communicated by nanonetworks to exchange information between different nanodevices [7].

The objective of this paper is to provide an overview of the IoNT system. It starts by providing an overview of the IoNT, its communication types, and network architecture. In addition, the paper involves an examination of applications that benefit from integrating IoT with nanotechnology. Challenges standing in the way of successful deployment of the IoNT are also discussed. In the end, since security is considered to be one of the main issues that face the IoNT system due to the large scale of nanosensors with limited computation capabilities and memory, we investigate the security of the IoNT system by discussing security goals, attack vectors, and security challenges.

The rest of the paper is organized as follows: Section 2 provides an overview of the IoNT system; the network architecture of the IoNT is presented in Section 3; Section 4 provides an overview of various applications of the IoNT; Section 5 discusses the challenges of IoNT systems; Section 6 presents security of the IoNT by discussing security goals, attack vectors, and security challenges; and Section 7 is the conclusion.

2. INTERNET OF NANO THINGS
The notion of nanotechnology was introduced by Richard Feynman in December 1959 [8]. The basic idea behind the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
ICCBDC'18, August 3–5, 2018, Barcelona, Spain
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6474-4/18/08…$15.00
https://doi.org/10.1145/3264560.3264570

expansion and practice of nanotechnology is miniaturization and production of devices in the scale of 1 to 100 nanometres [9]. Nanotechnology has resulted in new nanomaterials with new characteristics that help to develop novel nanodevices such as nanorouters and nanosensors [6].

Nanotechnology is considered to be the building block of the IoNT, which is comprised of nanoscale networks of physical objects to share information between each other using nano communication techniques. The concept of IoNT was presented by Ian F. Akyildiz and Josep Miguel Jornet from Georgia Institute of Technology [10]. They defined the IoNT as: "The Interconnection of nanoscale devices with existing communication networks and ultimately the Internet defines a new networking paradigm called the Internet of Nano-Things".

IoNT can be deployed by mixing nanodevices with existing technologies like IoT, sensors network, Cloud computing, etc. The development and widespread adoption of IoNT relies on processing capabilities, large storage at low costs, smart antennas and smart RFID tag technology. The IoNT has given birth of new domains like Internet of Bio-Nano Things (IoBNT) [11] and Internet of Multimedia-Nano Things (IoMNT) [12] which can add novel developments in healthcare and multimedia arenas.

3. NETWORK ARCHITECTURE OF IONT

The global IoNT market is expected to grow in the near future, attributed to growth in a number of connected devices, high demand for ubiquitous connectivity, high adoption of IoT among end-user industries, and need for better connectivity across the world [12]. IoNT nanosensors are connected to physical objects to collect, process, and share data with end users. However, the interconnection of nanomachines with current communication techniques need to develop new network architectures [13, 14].

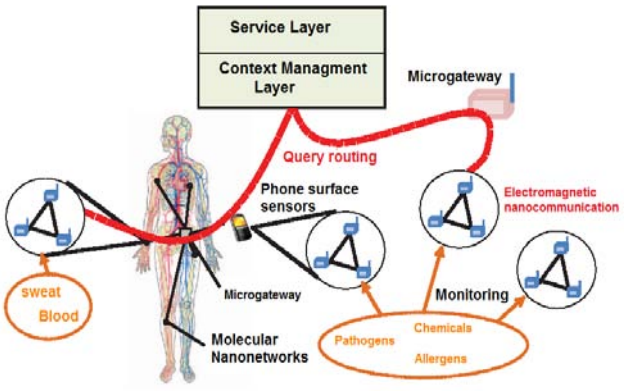

Figure 1. Network architecture of IoNT [15].

The components of the IoNT network is changed according to the context. However, there are essential elements for the network architecture of IoNT in various applications, as shown in Figure 1. These elements include:

- ***Nanonodes***: These nodes are considered to be the smallest and simplest nanomachines. Because of their limited energy, low memory, and limited communication capabilities, they can perform simple operations and transmit information over very short distances. Nanosensor nodes and nanomachines with communication capabilities are integrated into various objects such as human body [16].
- ***Nanorouters***: Compared to nanonodes, nanorouters have larger computational resources which are appropriate to combine information coming from different nanomachines. Nanorouters can also manage the behaviour of nanonodes by transmitting simple control commands such as sleep, on/off, read value, etc. Increasing the capabilities of these devices result in increasing their size which makes their deployment more difficult [2].
- ***Nano-micro interface devices***: These devices are used to combine the information collected from nanorouters to transport it to the microscale domain, and vice versa. Nano-micro interfaces are supposed to be hybrid devices that able to communicate in the nanoscale domain using both noncommunication techniques and traditional communication approaches in classical communication networks [17].
- ***Gateway*:** It is used to control the entire system remotely over the internet. For instance, in an intrabody network, the information received by an advanced cell phone from a nano-micro interface in the wrist can be forwarded to the healthcare provider [12].

4. APPLICATIONS OF IONT

IoNT has involved in several applications such as multimedia, military, industry, smart cities, agriculture, and health monitoring. This section gives an overview of common applications where IoNT can use nanotechnology to add more benefits to various domains, as shown in Figure 2.

4.1 Oil and Gas

Nanosensors can be used to enhance the discovery rates of the oil. They can travel through the pores of the rocks and help to find the oil bounded to the rocks. Although cross-well imaging tools add more impact to the field, their provided resolution is very low such that the location of the oil is identified using huge magnetic source and receiver to map the nanoparticles that are inserted using recycled water [18]. In IoNT, nanosensors interact and communicate with each other by molecular communication and the collected information can be conveyed in real-time using a nearby gateway. This allows the location of oil to be efficiently mapped without requiring a specific magnetic source and receiver [19].

4.2 Military

The war strategy has changed with the existence of new advanced biological and chemical weapons that make the difference in any battle. In the military, the IoNT can use nanosensors to discover the existence of a chemical composite in a concentration of even only one molecule. The composition of molecules of a room or the battlefield can be identified by nanosensors without the need for external tools such as the devices used for spectroscopy. In addition, nanosensors have the capability to identify the problems of very small cracks in bridges, civil structures, vehicles, textiles and rockets [6].

4.3 Agriculture

There are many successful scenarios where IoNT can improve the productivity of the agriculture. For instance, there are numerous types of nanoparticles that have proved its efficiency in pest management. Nanoparticles also can be used to control fungi in plants [20]. These particles can be embedded into a nanosensor and used to control and monitor the planting process using the IoNT. For example, the fertilizer can be sent out to the plant based

on monitoring conditions of the plant [21]. Moreover, the information collected regarding the infected plant can be transmitted to the owner to check the plants status and trigger the release of nanosensors. In brief, IoNT can enable precision farming that uses facilities of satellite communication, geographic information systems, and remote sensing to enhance the efficiency and productivity of the agriculture [19].

4.4 Smart Cities

The implementation of a smart city provides a smooth interaction and communication with home appliances, monitoring sensors, surveillance cameras, actuators, vehicles, and others. The roadmap of the smart city depends on geographical environments and people lifestyle. All communication technologies provided by the smart city can be used by anyone regardless of their economic condition [22]. With IoNT, nanosensors can be used to monitor and identify locations of pollution discovered in the air in high concentration and trigger nanosensors to clean up that specific location [23]. In addition, with the existence of a countless number of nanosensors, it can be used to collect huge amounts of real-time information to improve the quality of life and provide new services and applications.

4.5 Multimedia

Nanotechnology has offered new nonmaterial that can be used to manufacture a novel generation of miniature photodetectors and acoustic nano-transducers. This allows creating new multimedia content at the nanoscale dimension that can add more benefits to various multimedia applications such as ultra-high-resolution imaging of distant objects for satellite imaging and ultra-high-resolution imaging for crime scenes [24]. Increasing resolution and accuracy of visual and acoustic information is not an easy task, but with nano-cameras and nano-phones, this issue can be handled by enabling higher computational and storing capacities, higher quality image and audio sensing capabilities, and higher energy efficiency [6].

4.6 Health Monitoring

Nanosensors have several applications in health monitoring. Several parameters such as cholesterol, glucose, and sodium can be observed using nanosensors. Cancer-causing tumours and other harmful agents can be also detected by nanosensors [25, 26]. In addition, nanosensors can be used to fix the demyelinated neurons by finding the affected zone and employing a myelin sheath [27]. Although identifying the precise location to place the sheath is very difficult to know, IoNT nanosensors can relay the nerve impulse signal to the destination or towards the other end of the nerve [19].

4.7 Industry

IoNT can provide several benefits to the industry. It can improve the sensitivity of touch technology using air through nanosensors to identify movements of a particular figure in the air and translate it into signals [28]. Most industries use Radio Frequency Identification (RFID) tags to identify and monitor the production components, but RFID tags are mostly passive and require nearby readers to exchange information. While with IoNT, nanosensors can be used to transmit the information of the production line directly over the Internet. Also, Product Lifecycle Management (PLM) tool can be used to detect any unexpected action and trigger an alarm on the production line manager's personal device [29, 30].

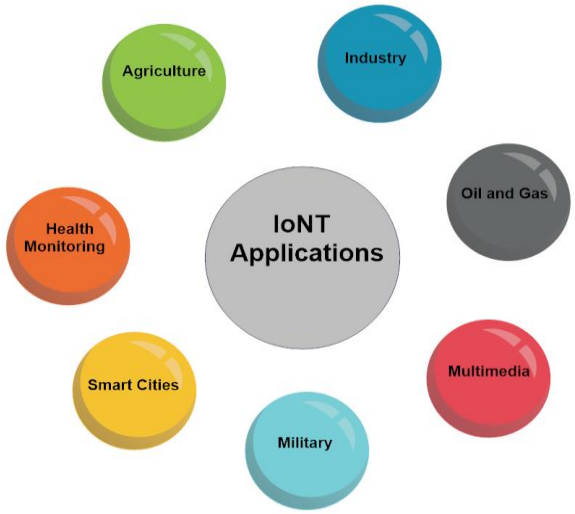

Figure 2. IoNT applications

5. CHALLENGES OF IONT

IoNT is considered to be the most miniaturized of nanosensor networks that have massive potential to be adopted in real-time applications. Although the IoNT provides unlimited benefits, it suffers some challenges that need to be handled to enable the IoNT to be an essential segment of mankind in the near future without any limitations. This section provides an overview of the most common challenges of the IoNT.

5.1 MAC Protocol for Nanomachines

Nanomachines transmit the information from the source to the destination using very short pulses. Nanonetworks cannot use Medium Access Protocol (MAC) for carrier sensing-based communication. This is because no carrier signal is used for sensing. Therefore, new MAC protocols need to be investigated for pulse-based transmissions of nanonetworks [31, 32]. Nanomachines are simple devices with limited capabilities so the new protocols should not be very complicated. The information is conveyed through very short pulses which decreases the likelihood of collisions between different nanonodes trying to access the channel at the same time. In addition, new MAC protocols should be designed to give maximum scalability, throughput, and fairness for nanomachines [33].

5.2 Bandwidth Constraints and Channel Capacity

Obviously, the need for more data grows every day, so that more bandwidth is needed. However, the available bandwidth is limited. This challenge can be addressed by converting to unexploited bands of the electromagnetic spectrum such as the terahertz band. The terahertz band provides a huge amount of bandwidth for very short ranges. Therefore, a large amount of channel capacity will be accessible for nanonetworks. However, nanomachines are simple devices with limited capabilities, so utilizing the entire channel efficiently by these nanomachines is not a simple task which will need more investigation [24].

5.3 Data Analysis

Current sensor networks collect data using a static tree in which each node senses the surroundings, collects relevant data and then passes it to the sink node in the tree. In IoNT scenario, there are a large number of nanosensors connected to the microgateway which can result in a significant concern related to data traffic [34].

In molecular and EM nanonetworks, data coming from different nanosensors are integrated using microgateway before transmitting it to the tree. Since data propagation is different between nanosensors, this leads to long delays for messages being delivered to the sink [15]. Therefore, an optimum time-delayed data fusion method must be implemented at the microgateway to process all information before transmitting it to the tree.

5.4 Security and Privacy

IoNT is being incorporated into most applications of our life such as phones, household appliances, sensors, vehicles, and large-scale infrastructure systems. These devices have their control and monitoring procedures digitized and connected to the Internet, which raises many security and privacy issues [35]. Our body which is attached to many nanosensors is now under attack. Critical data can be easily breached by the hacker as it is available via the Internet. This may lead to damage to victims including theft, spying, and manipulation of their data. Therefore, new security and privacy techniques are required to protect sensitive data collected by nanosensors [15].

The next section will focus on the security of the IoNT by highlighting security goals, attack vectors and security challenges of the IoNT system.

6. SECURITY OF IONT

Like all new technologies, security is one of the most difficult issues that face the adoption of the IoNT in our community. The attacker can now literally take your life, rather than just your money. Nanonetworks comprise of nanodevices that communicate together to exchange information. Vulnerabilities of nanonetworks can be exploited by attackers to use its sensitive data to perform malicious actions. This is because standard security techniques cannot be applied to nanonetworks that operate in the terahertz band. To secure the IoNT system, there is a need to develop new security solutions [16, 36].

In addition, one of the significant sources of the IoNT data is healthcare, which raises significant concerns about data privacy. Medical information should be protected from unauthenticated access which can have a serious effect on people's lives. Therefore, privacy challenges should be handled to ensure the appropriate use of the sensitive data collected from personal health monitoring devices [37].

According to F. Dressler and S. Fischer [21], attackers can exploit the IoNT data which include:

- Attack on private data such as biological data gathered by either in-body or wearable sensors;
- Disruption of medical applications such as dedicated drug delivery applications controlled by a wearable device;
- Modification of communication links at the nano communication level or at the gateway to the Body Area Network (BAN).

6.1 Security Goals of IoNT

Security of the IoNT system can be assessed by employing classical security and risk analysis measures [38]. Typical CIA (Confidentiality, Integrity, and Availability) security goals can be evaluated in the IoNT context [21].

- ***Confidentiality***: Messages exchanged between a sender and a receiver should be protected against any malicious or unauthenticated user [39]. In the IoNT system, confidentiality need not only to be guaranteed inside the BAN network but also when transmitting messages between various nanodevices [15]. For example, Advanced Encryption Standard (AES) and Rivest, Shamir, and Adelman (RSA) encryption techniques can be used to encrypt data within nanonetworks.
- ***Integrity***: The content of messages exchanged between a sender and a receiver should be protected against modification by an intruder without the receiver being able to track this modification [40]. In the IoNT system, integrity checks need to be applied not only on BAN nodes but also on the nanodevices and microgateway. The integrity checks can be carried out at each node involved in the message exchange between the originator and the (final) receiver [34].
- ***Availability***: A malicious user must not be capable of disrupting or harmfully affecting communication or quality of service provided by either nanodevices or nanonetworks. In the IoNT scenario, availability of the BAN network, in-body nano communication network, and gateway nodes should be maintained under all situations and conditions. Adaptive self-organizing solutions are needed to handle this issue [16].

6.2 Attack Vectors in IoNT

An attack vector is a method by which unauthorized access can be gained to a device or a network by a malicious user or an attacker. It tries to exploit the vulnerabilities in a device or a network [41]. There are several attack vectors associated with the IoNT system that need to be handled by implementing the required security measures to mitigate against.

- ***Internet Exposure:*** Although connecting nanodevices to the Internet helps to share information with each other and allow real-time applications, any device which connects to the Internet and accepts incoming traffic eventually comes under attack. Unlike the network server where a firewall can control how the host can be accessed, nanodevices are employed with limited computation capabilities and memory and without built-in security features that make it an easy target to various attacks coming from different locations over the Internet.
- ***Lack of Encryption*****:** Unfortunately, security is often an afterthought in the development lifecycle of IoNT devices. Encryption is missing from most nanodevices due to their small size and limited computation capabilities. Failure to encrypt sensitive data exchanged between nanodevices, whether on nanodevice itself or on nanonetworks will lead to several security issues especially when nanodevices become part of our bodies. Embedded cryptography such as cryptographic co-processors, which can address encryption and authentication of nanodevices, is required and securing data of nanodevices should be part of any design.
- ***Wearable Malware***: There is a rapid growth of wearable devices in different fields [42]. These devices include smart glasses and headgear, fitness trackers, wearable medical devices, smart watches, and smart clothing and accessories. Wearables devices might become attractive targets for malicious software, especially they use Bluetooth which uses frequency hopping whereby many devices can transmit a signal across the same frequency at the same time [43]. This increases the chances of signal interception by attackers and theft of sensitive information from these unencrypted feeds.
- ***Denial-of-service***: This is defined as any event that diminishes or eliminates the capacity of a network to perform its expected

function [44]. An attacker tries to affect the availability of a network that might be difficult to protect, as attackers might have sufficient energy to jam radio transmission or flood the communication channel with large amounts of molecules that destroy regular communication molecules.

- ***Water Resource Contamination***: Water is one of the essentials of our daily lives. This resource is vulnerable to bioterrorism attack. To monitor and maintain the quality of the water, a network of nanosensors could be released into the water to monitor and track the contingent presence of dangerous biological agents [45]. However, the attacker could release their own nanosensors along with the anthrax spores to create maximum damage.

6.3 Security Challenges in IoNT

IoNT introduces new security issues that need to be addressed to ensure successful deployment of the IoNT in various applications. This section provides an overview of the security challenges of the IoNT system.

- ***Key Management***: Distributing security keys is considered to be the root of nearly all key management systems. Keys can be distributed either by key pre-distribution before the deployment or pro-active in a sensor network before any data transmission occurs. It is essential to have the ability to revoke a key when it has been disclosed [43]. This issue is still one of the most challenging issues in sensor networks and IoNT systems. It is necessary to define standard procedures to create shared keys and define how keys can be revoked when necessary.
- ***Performance and scalability*:** IoNT security will create enormous performance and scalability issues. There will be severe resource limitations in nanomachines that make nano communication which is unmatched in current communication systems. Although the performance of cryptographic algorithms has been assessed in the sensor network, these results cannot be directly applied to the nanodomain due to different procedures of information processing [44]. In addition, energy consumption is another serious issue since communication systems like nano-tube based radios require significant power because of the cryptographic payloads they create [46]. Therefore, the performance of communication protocols and cryptographic techniques should be taken into consideration when developing practical applications.
- ***Access Control and Authentication*:** Authentication is typically achieved using traditional symmetric or asymmetric cryptography. Biochemical cryptography is a new and still unexplored field which uses biological molecules like DNA/RNA evidence to encrypt information and protect the confidentiality and integrity of data. Although this cryptography scheme opens various novel application domains, it leads to new issues related to the communication system. Complex molecules can spontaneously respond within the system which results in modifications out of the control of the nanomachinery. Therefore, the biochemical processes involved in the system need to be better understood [44].
- ***Secure Localization***: Some applications that use nano communication need the localization of nanomachines to complete their operations. The difference in demands between classical sensor networks, using other coordinate systems, and nanodevices make generating an absolute positioning with nanoscale resolution difficult to realize, but relative positioning might be more relevant. This links directly to security to permit only nearby nanomachines to communicate and prevent remote attackers from interfering [47].
- ***Intrusion Detection***: Some attacks typically cannot be handled by cryptography. For instance, denial-of-service attacks that try to disrupt the availability of a system might be difficult to protect against in a nano communication network. This is because attackers might have the necessary energy to jam radio transmission or flood the communication channel with huge amounts of molecules that destroy regular communication molecules. 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 [48]. Therefore, it is critical to establish new intrusion detection systems that are able to detect and react to attacks efficiently in nanonetworks.

7. CONCLUSION

The development of nanomachines with communication capabilities and their interconnection using nanonetworks has enabled the concept of IoNT. This new networking paradigm has a significant effect on several applications in our life, especially in health monitoring, agriculture, military, and smart cities. The objective of this paper was to provide an overview of the IoNT system by highlighting its communication types and network architecture. Various applications and challenges of the IoNT system have discussed. Since security is one of the main issues that face the IoNT due to its large number of nanosensors with limited computation capabilities that do not allow applying sophisticated security algorithms, we have investigated the security of the IoNT system by discussing security goals, attack vectors, and security challenges. In summary, although the opportunities and applications of IoNT are countless, there is a need to integrate hardware and software solutions to the existing setup in a seamless manner to address challenges facing its positive deployment, especially for security issues.

8. ACKNOWLEDGMENTS

We acknowledge Egyptian cultural affairs and missions sector and Menoufia University for their scholarship to Hany Atlam that allows the research to be funded and undertaken.

9. REFERENCES

[1] H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, “Integration of cloud computing with internet of things: challenges and open issues,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 670–675.

[2] A. Nayyar, V. Puri, and D.-N. Le, “Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology,” Nanosci. Nanotechnol., vol. 7, no. 1, pp. 4–8, 2017.

[3] K. Ashton, “That ‘Internet of Things’ Thing,” RFID J., p. 4986, 2009.

[4] M. Abdur, S. Habib, M. Ali, and S. Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, 2017.

[5] H. F. Atlam, R. J. Walters, and G. B. Wills, “Fog Computing and the Internet of Things: A Review,” Big Data Cogn. Comput., vol. 2, no. 10, pp. 1–18, 2018.

[6] H. E. El-din and D. H. Manjaiah, “Internet of Nano Things and Industrial Internet of Thing,” in Internet of Things: Novel Advances and Envisioned Applications, vol. 25, 2017, pp. 109–123.

[7] H. F. Atlam, R. J. Walters, and G. B. Wills, “Intelligence of Things: Opportunities & Challenges,” in IEEE 2018 Cloudification of the Internet of Things (CIoT).

[8] R. P. Feynman, “There â€TM s Plenty of Room at the Bottom,” 1961.

[9] A. Nayyar, V. Puri, and D.-N. Le, Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology, Nanosci. Nanotechnol., vol. 7, no. 1, pp. 4–8, 2017.

[10] I. F. Kyildiz and J. O. M. I. J. Ornet, “The Internet of Nano-Things,” IEEE Wirel. Commun., vol. 17, no. 6, pp. 58–63, 2010.

[11] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, “The internet of bio-nano things,” IEEE Commun. Mag., vol. 53, no. 3, pp. 32–40, 2015.

[12] J. M. Jornet and I. F. Akyildiz, “The internet of multimedia Nano-Things,” Nano Commun. Netw., vol. 3, no. 4, pp. 242–251, 2012.

[13] K. Agarwal, K. Agarwal, and S. Agarwal, “Evolution of Internet of Nano Things (IoNT),” Int. J. Eng. Technol. Sci. Res., vol. 4, no. 7, pp. 274–277, 2017.

[14] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, “An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things,” in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), 2017, pp. 254–260.

[15] S. Balasubramaniam and J. Kangasharju, “Realizing the Internet of Nano Things: Challenges, Solutions, and Applications,” EEE Comput. Soc., pp. 62–68, 2013

[16] O.-M. E. and M. M., “The Future of Healthcare: Nanomedicine and Internet of Nano Things,” Folia Medica - Fac. Med. Univ. Saraeviensis, vol. 50, no. 1, pp. 23–28, 2015.

[17] F. Al-Turjman, “A Cognitive Routing Protocol for Bio-Inspired Networking in the Internet of Nano-Things (IoNT),” Mob. Networks Appl., pp. 1–15, 2017.

[18] B. Usibe and A. Menkiti, “Development and Analysis of a Potential Nanosensor Communication Network Using Carbon Nanotubes,” Int. J. …, vol. 3, no. 1, pp. 4–10, 2013.

[19] P. Kethineni, “Applications of internet of nano things: A survey,” 2017 2nd Int. Conf. Converg. Technol., pp. 371–375, 2017.

[20] H. T. Gul, S. Saeed, F. Zafar, A. Khan, and S. A. Manzoor, “Potential of Nanotechnology in Agriculture and Crop Protection : A Review,” Appl. Sci. Bus. Econ., vol. 1, no. 2, pp. 23–28, 2014.

[21] 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, 2015.

[22] a Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.

[23] M. N. Kamel Boulos and N. M. Al-Shorbaji, “On the Internet of Things, smart cities and the WHO Healthy Cities,” Int. J. Health Geogr., vol. 13, no. 1, pp. 1–6, 2014.

[24] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, “XACML for Building Access Control Policies in Internet of Things,” in in Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), 2018, pp. 253–260.

[25] I. F. Akyildiz and J. M. Jornet, “Electromagnetic wireless nanosensor networks,” Nano Commun. Netw., vol. 1, no. 1, pp. 3–19, 2010.

[26] N. Rikhtegar and M. Keshtgary, “A Brief Survey on Molecular and Electromagnetic Communications in Nano-Networks,” Int. J. Comput. Appl., vol. 79, no. 3, pp. 16–28, 2013.

[27] S. Al-Arif and N. Quader, “Sensor based autonomous medical nanorobots: A cure to demyelination,” J. Sel. Areas Nanotechnol., pp. 10–15, 2011.

[28] K. Dabhi and A. Maheta, “Internet of Nano Things-The Next Big Thing,” Int. J. Eng. Sci. Comput., vol. 7, no. 4, pp. 10602–10604, 2017.

[29] M. U. Farooq and M. Waseem, “A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT),” Int. J. Comput. Appl. (0975 8887), vol. 113, no. 1, pp. 1–7, 2015.

[30] K. Huang and Z. Wang, “Terahertz terabit wireless communication,” IEEE Microw. Mag., no. June, pp. 108–116, 2011.

[31] J. M. Jornet and I. F. Akyildiz, “Graphene-based nano-antennas for electromagnetic nanocommunications in the terahertz band,” in Proceedings of the Fourth European Conference on Antennas and Propagation, Barcelona, Spain, 2010, pp. 1–5.

[32] M. Rosenau da Costa, O. V. Kibis, and M. E. Portnoi, “Carbon nanotubes as a basis for terahertz emitters and detectors,” Microelectronics J., vol. 40, no. 4–5, pp. 776–778, 2009.

[33] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, “Blockchain with Internet of Things: Benefits, Challenges, and Future Directions,” Int. J. Intell. Syst. Appl. (IJISA), Vol.10, No.6, pp. 40-48, 2018.

[34] 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.

[35] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, “Developing an adaptive Risk-based access control model for the Internet of Things,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 655–661.

[36] I. Lakshmi, “Interfacing In-Body Nano Correspondence with Form Region Networks : Tests and Chances of the Web for

Nano Things," Int. J. Comput. Sci. Mob. Comput., vol. 5, no. 12, pp. 182–196, 2016.

[37] N. A. Ali and A. Ain, "Internet of Nano-Things Network Models and Medical Applications," 2016 Int. Wirel. Commun. Mob. Comput. Conf., pp. 211–215, 2016.

[38] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," I.J. Comput. Netw. Inf. Secur., no. January, pp. 26–35, 2018.

[39] C. Maple, "Security and privacy in the internet of things," J. Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[40] X. Li, H. Wang, Y. Yu, and C. Qian, "An IoT Data Communication Framework for Authenticity and Integrity," Proc. Second Int. Conf. Internet-of-Things Des. Implement. - IoTDI '17, pp. 159–170, 2017.

[41] M. L. Hale and S. Hanson, "A Testbed and Process for Analyzing Attack Vectors and Vulnerabilities in Hybrid Mobile Apps Connected to Restful Web Services," Proc. - 2015 IEEE World Congr. Serv. Serv. 2015, pp. 181–188, 2015.

[42] H. Chen et al., "Wearable and robust triboelectric nanogenerator based on crumpled gold films," Nano Energy, vol. 46, no. January, pp. 73–80, 2018.

[43] R. Bouhenguel, I. Mahgoub, and I. Mohammad, "Bluetooth security in wearable computing applications," 2008 Int. Symp. High Capacit. Opt. Networks Enabling Technol. HONET 2008, pp. 182–186, 2008.

[44] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," Nano Commun. Netw., vol. 3, no. 3, pp. 151–160, 2012.

[45] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in Bio-NanoThings communication networks," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 4, pp. 665–676, 2016.

[46] B. Atakan and O. Akan, "Carbon nanotube-based nanoscale ad hoc networks," IEEE Commun. Mag., vol. 48, no. 6, pp. 129–135, 2010.

[47] S. Brands and D. Chaum, "Dist ance-Bounding Protocols," in Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Vol. LNCS 765, Lofthus, Norway, 1994, pp. 344–359.

[48] 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., pp. 1238–1246, 2008.