International Journal of Electronic Devices and Networking

E-ISSN: 2708-4485
P-ISSN: 2708-4477
IJEDN 2022; 3(2): 36-42

www.electronicnetjournal.com
Received: 06-05-2022
Accepted: 07-06-2022

Sreelakshmi Manojkumar
School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Correspondence
Sreelakshmi Manojkumar
School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Security and possible applications towards internet of nano things in near future

Sreelakshmi Manojkumar

Abstract
The current situations with future guarantees of the Internet of Nano-Things (IoNT) are broadly audited and a definite informations are introduced. From the interconnection of nano machines with the Internet arose the idea of Internet of Nano Things (IoNT).The main objective of this paper include the detailed view of IoNT, application areas and also the methods to overcome existing challenges and make use of IoNT in the future. With the evolution of IoT, it extended to collaborate with the fields of Nanotechnology resulting in IoNT. The significant topics of IoNT could be discussed as data delivery, caching, energy consumption. The very combination of Internet of Things (IoT) and Nanotechnology, it involves a system of small devices to transfer data over a network. What makes the difference between IoT and IoNT is that in the latter case, devices connected within it are small enough to be termed on a nanoscale. Internet of Nano Things promises its application in number of areas such as healthcare, agriculture, environmental monitoring, food products quality control, smart homes and factories and many more. Since security is considered to be one of the most issues of IoNT, the discussion for security goals, attack vectors and security challenges as well as the future is presented in the paper.

Keywords: Internet of things (IOT), internet of nano things (IoNT), vectors, nanotechnology, nanosensors, sensors, nano communication

1. Introduction
The Internet of nano things involves the very process of embedding nano-sensors in the devices. This, with the help of internet helps to communicate through the nanotechnology network. This is a futuristic network where individual nano-things (NTs) perform straightforward calculations, correspondence, discernment and activation to fill confounded roles. Due to their small size, NTs will be able to reach inaccessible places and detect even limited quantities of substances to be identified. The rising interest for universal and omnipresent frameworks has spawned a significant amount of research activity in the field of nanoscale networking [11]. With the help of Internet of Nano things, many of the dangerous things happening around us could be prevented. The Internet of Things (IoT) is growing in popularity every day, thanks to existing and emerging wireless telecommunications technologies. The Internet of Things (IoT) has the capacity to connect and communicate with all things in our environment via wired or wireless networks. The Internet of Nano Things (IoNT), which is based on the interconnection of nanoscale devices, was inspired by the features of recently researched nanomaterials such as graphene. As of late, the idea of IoT has been updated considering novel examination propels made in the area of nanotechnology and correspondence designing, which empower the advancement of organizations of inserted figuring gadgets, based on nano materials, for example, graphene or meta materials, having scales going from one to a couple hundred nanometers, called nanothings. With the evolution of IoNT, examination inside the space of Nano correspondence has moreover exaggerated 10 times with partner objective to make new principles for Nano gadgets to talk among each other and may even be conveyed in various applications. IoNT can contain little sensors associated with each unique through Nano organizations to get data from objects. Along these lines, progressively IoNT things can open new entryways of examination inside the space of Nano Sensors, Nano correspondence what's more, Nano Devices. The point of this work is to examine best in class and break down patterns in the utilization of IoNT, its application and future difficulties in various fields. On the off chance that we consider that the IoNT depends on the utilization of nanotechnology for the equipment that will work in an organization, it is feasible to affirm that the IoNT is a situation where creatures, individuals or articles are totally associated or have some remarkable identifiers permitting these to cooperate overall.

We can derive that the IoNT is the "expansion of IoT in which it fuses Nano-sensors in different articles related to the utilization of Nano-organizations". That is, the intention is the capacity to interconnect various kinds of gadgets created at a Nano-scale in an interchange organization, all centred around setting up a usefulness around the assortment of information and the exhibition of errands in spots of difficult access. The IoNT foundation relies upon the space of activity and required transfer speed needed by specific application. The upgrade and wide reach reception of IoNT relies upon preparing capacities, enormous capacity at low expenses, shrewd radio wires and Smart RFID label innovation. The improvement of Nanotechnologies, nano machines, Internet of Things (IoT), Internet of Nano Things (IoNT) will incredibly affect progressed advancement in pretty much every field in not so distant future. In this paper, all around study concerning Internet of Nano Thing (IoNT) is presented which is seen as next formative development in universe of nanotechnology in any case. The goal of this paper is to give an outline of the IoNT framework. Since security is viewed as one of the principle of IoNT framework because of the huge size of nanosensors with restricted calculation capacities and memory, we examine the security of the IoNT framework by talking about security objectives, assault vectors, and security challenge.

2. IoNT Network Architecture

The interconnection of nanomachines with existing correspondence organizations and at last with the help of internet requires the improvement of new organization structures. The IoNT nanosensors are associated with actual items to gather, interaction, and offer information with end clients. Notwithstanding, the interconnection of nanomachines with current correspondence strategies need to foster new organization models. The Internet of Nano Things (IoNT) Network Architecture contains Nano hubs that play out a variety of tasks like estimation and transmission of data with short distance and less memory. Nano routers can go about as aggregator to gather data from nano nodes. Nano-Micro interface gadgets play out the errand of collection of information appearance from nano-routers and afterward send it to the small size as well as the other way around. The correspondence between nano gadgets is through a standard correspondence network with customary association shows. The Gateway enables the regulator of fundamental nano network. A part of the Applications needed for IoNT are gas revelation structure, so reduced Nano sensor can recognize the gas spillage and submit you a blast alert for the fundamental exercises. Nano-Micro interface gadgets play out the undertaking of gathering of information appearance from nano-switches and from that point confer it to the little size similarly as the opposite way around. However in these context it is necessary to understand different elements of IoNT which are:

1) Nanonodes

Nanonodes are viewed as the smallest and easiest nano machines which perform different errands like calculation and transmission if the information over brief distances and have less memory.

2) Nano-Routers

Nano-switches have colossal computational force when showed up contrastingly corresponding to nanonodes and they go about as aggregators of data coming from nanonode focuses. Nano-routers moreover expect earnest part in controlling nanonodes by profession control orders.

3) Nano-micro Interface Devices

These gadgets play out the assignment of total of data coming from nano-routers and send it to the microscale as well as the other way around. They go about as combination contraptions to pass on in nanoscale using nano correspondence strategies and moreover with ordinary correspondence networks with customary association shows.

4) Gateway

It draws in the controller of whole nano things network over the Internet. For example, considering Body Sensor Network-With the usage of Gateway all the sensor data from the Human Body can be gotten to any place and any spot through experts over Internet.

3. IoNT and it's application in different fields

1) Healthcare

Consistent populace development impacts of medical care requests also, needs for new, further developed logical arrangements. Traditional method of giving the medical care administrations could be exceptionally hearty. It requires new worldview and innovation for more viable arrangements. Quick improvement data and nano innovations change the medical care framework altogether. It provides for the medical services framework a new, worldwide space – Internet of Nano Things (IoNT) also, nanomedicine. For Example: The biological embedded computing device is based on biological cells and their functionalities in accordance with biochemical areas, which unquestionably guarantees the primary reason for detecting and actuation in the intrabody, and furthermore helps in the ecological control of toxins and pollution [10].

2) Agriculture

All through the last decade, exactness agriculture has filled in im-portance to satisfy the growing food need and assurance legitimacy of developing. Farmers will be involved in these nanosensors and they will be crucial for the development of the country. The sensors help farmers to check grass monitoring, and field condition, which helps farmers to predict and till the field and use pesticides and insectoids in the agricultural field[12]. Today, pushes in the Internet of Things (IoT) perspective have progressed the use of Wireless Sensor Networks (WSN) for exactness developing. Regardless, continuous mechanical headways recommend that use of Nanotechnology might perhaps furthermore chip away at the developing productivity. Also another thing to be understood is that the nanoparticles would help to control the excessive fungi growth in plants.

3) Military

The contention strategy has changed with the presence of new advanced natural and compound weapons that have the impact in any battle. In the military, the IoNT can use

nanosensors to discover the presence of an engineered composite in an assembly of even only a solitary iota. The sythesis of molecules of a room or the disaster area can be recognized by nanosensors without the necessity for outside gadgets, for instance, the contraptions used for spectroscopy. In addition, nanosensors have the ability to recognize the issues of minuscule breaks in ranges, normal plans, vehicles, materials and rockets. The significant forward leap in nanotechnology may have a high potential to impact military capabilities. Key capabilities include performance and energy-efficient materials, high-resistance materials and coatings for platforms and weapons such as nano armour, nanomedical warfare of the future: countering chemical and biological warfare such as war spies, antitoxin and nanofingerprinting, surveillance, autonomous vehicles and mini-satellites [12].

4) Smart Homes

Nowadays, we are well equipped with smart home services however, implementation of IoNT would, to a great extent increase the usefulness of smart home and its offer to the end client. It's nanosensors are so efficient that more information can be gathered and over a more extensive scope of factors. The information gathered can be super-fine and granular. For example, suppose there happens to be a gas break ; during such incident, the nano sensors can assist us with distinguishing gas holes and ready alert house owners a long time before any genuine damage occurs for their property. Furthermore, nano sensors could be utilized for environment control or security.

5) Environmental Monitoring

The utilization of nanosensors in Environmental Monitoring through organization in open areas like Airports, Hotels and Restaurants, Railway Stations, Bus Stops and other public places live and continuous observing of Traffic, Air Pollution, Temperature Monitoring is accomplished efficiently.

6) Multimedia

It centers around the development of gadgets, for example, photograph identifiers and acoustic nano-transducers to deliver media content with high Resolution. The nano-interactive media frameworks have their concentration in different fields like wellbeing, organic assaults, measurable science, and modern cycle control. Expanding goal and exactness of visual and acoustic data is anything but a simple errand, however with nano-cameras and nano-telephones, this issue can be dealt with by engaging higher computational and taking care of cut off points, more noteworthy picture and sound recognizing capacities, and higher energy efficiency.

7) Food Packaging

The nanotechnology field has risen steeply over the past period and there are a few partnerships which are centering in the making of new types of nano estimated substance. Nonetheless, one industry which is stream to get on to this is the food business and this isn't unexpected as the public reference for regular food items has generally restrained the execution of arising food innovations and undeniably the most dynamic space of food nano science examination and extension is wrapping. In the wake of presenting nano material mixtures like SiO2, TiO2 and KMnO4 the food bundling fixing can be improved extraordinarily. Nanosensors can show the freshness status of food in real-time, which helps determine the exact expiry date. Nanosensors can be utilized for product tracking, brand protection and verification of archives such as passports [13].

4. Challenges of IoNT Systems

1) Privacy and Security

Clients of Internet of Nano Things framework should be educated with respect to who approaches their information and how their information will be utilized. This is because, since nanodevices gather huge volumes of classified information, concerns in regards to protection and security should be looked after. Additionally, the gathered information should be put away in a safe area with encryption and top tier network security. At whatever point left unsteady, cybercriminals can illegally get to this restricted data. Hence, IoNT engineers need to ponder these issues before the huge assembling and utilization of IoNT devices.

2) Compatibility

While making clinical nanosensors, the developers need to ensure that these nanosensors will not have any coincidental impacts on a patient's body. Also, architects and engineers might need to discover and investigate a wide scope of materials that can be viable with the human body. Moreover, discovering such materials will require broad testing, making the whole cycle tedious just as mistake inclined.

5. Invasion vectors In IoNT

The means by which an aggressor can get unapproved permission to a PC or association to pass on a payload or harmful outcome is called an invasion vector. Or in other words, admittance to a PC or organization to convey a payload or noxious result is called an invasion vector.

Assault vectors can be taken advantage to access delicate information, by and by recognizable data and other touchy data that would bring about an information break. It attempts to take advantage of the weaknesses in a gadget or an organization. There are a few invasion vectors related with the Internet of Nano Things framework that should be taken care of by executing the necessary safety efforts.

1) Internet Exposure

Any gadget which associates with the Internet and acknowledges approaching traffic ultimately are prone to any kind of attacks. Nano devices are utilized with restricted calculation abilities and memory and without worked in security includes that make it an obvious objective to different assaults coming from various areas over the Internet.

2) Lack of Encryption

It is to be understood that security is frequently a reconsideration in the improvement lifecycle of Internet of Nano Things devices. Encryption is absent from most nano devices because of their little size and restricted calculation abilities. The inability to encrypt information exchanged between nano devices, regardless of whether on nano device itself or on nano organizations will prompt a few security issues particularly when nano devices become part of our bodies. Installed cryptography, for example, crypto realistic

co-processors, which can address encryption and confirmation of nano devices, is required and getting information of nano devices is essential for any plan.

3) Denial of Service

A kind of digital attack, where a harmful performer means to convey a PC or other contraption blocked off to its normal customers by barging in on the device's average working is called Denial of Service. Here, the attacker tries to influence the accessibility of an organization that may be hard to ensure, as aggressors may have adequate energy to stick radio transmission or flood the correspondence channel with a lot of atoms that annihilate standard correspondence particles.

6. Security in nano-things

IoNT is helpless against a wide range of assaults, either physical or through remote advances. The assaults can happen to get private information through the burglary of sensors, interfere with applications controlled using PCs or change the correspondence joins in the nano-networks. These gadgets have their control and checking methods digitized and associated with the Internet, which raises numerous security and protection issues. Perhaps the main difficulties because of the development of the Internet of Nano Thing market, is identified with the security of information imparted over the Internet. The Internet of Nano Things is powerless against a wide range of assaults, either physical or through remote advancements, considering that this sort of gadget doesn't meet with consistent watchfulness. The assaults can happen to procure private information through the burglary of sensors, intrude on applications controlled using PCs, or alter the correspondence joins in the nano networks. The security targets are a progression of ideas that comprises privacy, honesty, and accessibility. Whenever nano specialized devices are combined with IoT, an ordinary sensor network security issues are confronted. The reach for an assailant, especially entryway center points and the blend of PDAs opens up absolutely new attack vectors. Also, the usage of these associations for social event extraordinarily private information going from region information to physiological data makes these associations a significant target for dangerous customers. Thus, new security and protection procedures are needed to secure touchy information gathered by nanosensors.

7. Objectives behind IoNT

1) Availability

A malicious client should not be equipped for disturbing or destructively influencing correspondence or nature of administration gave by either nano devices or nano networks. In this situation, the A noxious client should not be equipped for disturbing or destructively influencing correspondence or nature of administration gave by either nano gadgets or nano networks. Versatile self - sorted out arrangements are expected to deal with this issue.

2) Integrity

The messages traded between a sender and a beneficiary ought to be ensured against alteration by an intruder without the recipient having the option to follow this alteration. In the Internet of Nano Things framework, uprightness checks should be applied on BAN hubs as well as on the nano gadgets and miniature passage. The respectability checks can be done at every hub engaged with the message trade between the originator and the receiver.

3) Confidentiality

An assailant should not have the choice to get to the substance of messages exchanged between a sender and a gatherer. In our setting, this infers that characterization need not only be ensured inside the Body Area Network, e.g., using encryption systems, for instance, the striking AES or RSA estimations., and inside the In-Body Nano Communication association, e.g., contingent upon biochemical cryptography, yet essentially moreover when moving messages using a doorway system interconnecting the two universes. Obviously, security associate helpfulness is required start with cryptographic techniques for encryption and progressed stamps yet furthermore for check as a base convenience.

8. Security mechanisms OF IoNT

1) Key Management

The process by which foundation to symmetric keys is laid is Key Management. Coursing security keys is seen as the establishment of practically all key organization systems. Keys can be spread either by key pre-allocation before the sending or good for dynamic in a sensor network before any data transmission occurs. It is principal drop a vital when it has been uncovered. This issue is at this point quite possibly the most troublesome issues in sensor organization besides, IoNT structures.

2) Access Control and Authentication

Verification is an essential to ensure the goal of privacy. Every one of the messages that need to be sent to a nano-correspondence framework should pass through a passage and be validated. Confirmation is ordinarily accomplished utilizing conventional symmetric or unbalanced cryptography. Biochemical cryptography is a new and still neglected field which utilizes natural particles like DNA/RNA proof to scramble data and secure the secrecy and uprightness of information. This cryptography plot opens different novel application spaces, it prompts new issues identified with the correspondence framework. The mind boggling particles can unexpectedly react inside the framework which brings about alterations out of the control of the nano apparatus. In this manner, the biochemical cycles included in the framework should be better perceived.

3) Secure Localization

In IoNT, a significant number of the applications should know the area of the nano-sensors to perform explicit positions. A few applications that utilize nano correspondence need the confinement of nano machines to finish their tasks. The distinction in requests between old style sensor organizations, utilizing other facilitate frameworks, and nano gadgets make producing a flat out situating with nanoscale goal hard to acknowledge, however relative situating may be more relevant. This connections straightforwardly to security to allow just close by nano machines to impart and forestall remote attackers from meddling.

4) Performance and Scalability

The security and protection in the nano-correspondence frameworks present huge difficulties with respect to the exhibition and versatility of the taking part hubs. IoNT protections will make huge execution and versatility issues. There will be extreme asset impediments in nano machines that make nano correspondence which is unrivaled in current correspondence frameworks. The presentation of cryptographic calculations has been evaluated in the sensor organization, these outcomes can't be straightforwardly applied to the nano space because of various methods of data preparing.

Also, energy utilization is one more difficult issue since correspondence frameworks like nano-tube based radios require huge force as a result of the cryptographic payloads they make. Along these lines, the presentation of correspondence conventions and cryptographic methods ought to be thought about when creating viable applications. Further, researchers re suggest to refer essential work on IoTs and its applications in [11-46].

9. Conclusion

The idea of IoNT was empowered by the improvement of nanomachines with correspondence limits and their interconnection using nanonetworks. IoNT presents capacities and conceivable outcomes to work on numerous parts of individuals' lives. Its principle characteristics are centered around observing and analytic administrations, which would help and improve dynamic and results in different fields of utilization. It gives an extraordinary assortment of nano-gadgets with different limits autonomous of the kind of engineering that is needed, to get information of items, individuals, creatures, plants, and so on. Also, there is no homogeneity between the advancement of equipment and programming. The equipment propels quicker than the product, accordingly, the inadequacies in the security and protection of the information. There are many difficulties that IoNT faces, however nanotechnology gives different fields of study that develop with expanding power and increment the conceivable outcomes of tackling current inadequacies. Yet, the momentum market guides examination to specific circumstances that typically don't benefit the majority of the populace. The motivation behind this paper was to give an outline of the Internet of Nano Things (IoNT) framework by featuring its correspondence types and organization design, and communications challenges just as different applications and difficulties of the IoNT framework have talked about. We have additionally examined the Internet of Nano Things (IoNT) security instruments, attack vectors in Internet of Nano Things (IoNT), security point. The advancement of Nanotechnologies and Internet of Nano things (IoNT) is relied upon to enormously affect progressed advancement in each field.

10. References

1. Nikhat Akhtar, Yusuf Perwej. The internet of nano things (IoNT) existing state and future Prospects. GSC Advanced Research and Reviews. 2020;5(2):131-150. ff10.30574/gscarr.2020.5.2.0110ff. ffhal-03226642
2. Nayyar V Puri, DN Le. Internet of Nano -Things Chen CJ Y Haik, Chatterjee J. Development of nanotechnology for biomedical applications, in Conference, Emerging Information Technology. IEEE; c2005 .p. 4-12.
3. Balasubramaniam S, Kangasharju J. Realizing the internet of nano things: challenges, solutions, and applications. Computer. 2013;46(2):62-68.
4. Taniguchi N. On the basic concept of nano-technology, in: Proceeding of the International Conference on Production Engineering; c1974.
5. Ali NA, Ain A. 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; c2015. p. 9-14.
6. Akyildiz IF, Jornet JM. The internet of nano-things. IEEE Wireless Communications. 2010;17(6):58-63.
7. Jarmakiewicz J, Parobczak K. On the Internet of Nano Things in healthcare network. In Military Communications and Information Systems (ICMCIS); c2016 May.
8. Hale ML, Hanson S. 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; c2015. p. 181-188.
9. Pattar A, Lagashetty A, Savadi A. An Anamnesis on the Internet of Nano Things (IoNT) for Biomedical Applications. ICCCE; c2018. p. 211-218. Doi: 10.1007/978-981-13-0212-1_22
10. Sharma D, Tyagi AK. Preserving Privacy in Internet of Things (IoT)-Based Devices. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems; c2023. p. 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_63
11. George TT, Tyagi AK. Reliable Edge Computing Architectures for Crowdsensing Applications, 2022 International Conference on Computer Communication and Informatics (ICCCI); c2022. p. 1-6. Doi: 10.1109/ICCCI54379.2022.9740791.
12. Rekha G, Tyagi AK, Anuradha N. Integration of Fog Computing and Internet of Things: An Useful Overview. In: Singh P, Kar A, Singh Y, Kolekar M, Tanwar S. (eds) Proceedings of ICRIC 2019. Lecture Notes in Electrical Engineering; c2020. p. 597. Springer, Cham. https://doi.org/10.1007/978-3-030-29407-6_8
13. Mishra S, Tyagi AK. The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham; c2022. https://doi.org/10.1007/978-3-030-87059-1_4
14. Sheth HSK, Tyagi AK. Mobile Cloud Computing: Issues, Applications and Scope in COVID-19. In: Abraham, A., Gandhi, N., Hanne, T., Hong, TP., Nogueira Rios, T., Ding, W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems; c2022. p. 418. Springer, Cham. https://doi.org/10.1007/978-3-030-96308-8_55
15. Tyagi Amit Kumar, Shamila M. Spy in the Crowd: How User's Privacy Is Getting Affected with the

Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India; c2019 February 26-28.
16. Tyagi Amit Kumar. Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India; c2019 February 26-28.
17. Reddy KS, Agarwal K, Tyagi AK. Beyond Things: A Systematic Study of Internet of Everything. In: Abraham A., Panda M., Pradhan S., Garcia-Hernandez L., Ma K. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2019. Advances in Intelligent Systems and Computing; c2021. p. 1180. Springer, Cham. https://doi.org/10.1007/978-3-030-49339-4_23
18. Tyagi AK, Rekha G, Sreenath N. Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. Learning and Analytics in Intelligent Systems; c2020. p. 3. Springer, Cham. https://doi.org/10.1007/978-3-030-24322-7_50
19. Tyagi K, Goyal D. A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things, 2020 5th International Conference on Communication and Electronics Systems (ICCES); c2020. p. 386-394. Doi: 10.1109/ICCES48766.2020.9137886.
20. Tyagi Amit Kumar, Nair Meghna Manoj. Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future, Journal of Information Assurance & Security (JIAS). 2020;15:4.
21. Malik S, Tyagi AK, Mahajan S. Architecture, Generative Model, and Deep Reinforcement Learning for IoT Applications: Deep Learning Perspective. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham; c2022. https://doi.org/10.1007/978-3-030-87059-1_9
22. Nair MM, Kumari S, Tyagi AK. Internet of Things, Cyber Physical System, and Data Analytics: Open Questions, Future Perspectives, and Research Areas. In: Goyal D., Gupta A.K., Piuri V., Ganzha M., Paprzycki M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems; c2021. p. 166. Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_36
23. Tyagi AK, Agarwal K, Goyal D, Sreenath N. A Review on Security and Privacy Issues in Internet of Things. In: Sharma H., Govindan K., Poonia R., Kumar S., El-Medany W. (eds) Advances in Computing and Intelligent Systems. Algorithms for Intelligent Systems. Springer, Singapore; c2020. https://doi.org/10.1007/978-981-15-0222-4_46
24. Deshmukh N Sreenath, Tyagi AK, Jathar S. Internet of Things Based Smart Environment: Threat Analysis, Open Issues, and a Way Forward to Future, 2022 International Conference on Computer Communication and Informatics (ICCCI); c2022. p. 1-6. Doi: 10.1109/ICCCI54379.2022.9740741.
25. Amit Kumar Tyagi, Ajith Abraham. Internet of Things: Future Challenging Issues and Possible Research Directions, International Journal of Computer Information Systems and Industrial Management Applications. ISSN 2150-7988. 2020;12:113-124.
26. Madhav AVS, Tyagi AK. Explainable Artificial Intelligence (XAI): Connecting Artificial Decision-Making and Human Trust in Autonomous Vehicles. In: Singh PK, Wierzchoń ST, Tanwar S, Rodrigues J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems; c2023. p. 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_10
27. Nair MM, Tyagi AK. Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri D, Mandal JK, Sakurai K, De D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, 2022, 481. Springer, Singapore. https://doi.org/10.1007/978-981-19-3182-6_19
28. Tyagi A, Niladhuri S, Priya R. Never Trust Anyone: Trust-Privacy Trade-offs in Vehicular Ad-Hoc Networks. Journal of Advances in Mathematics and Computer Science. 2016;19(6):1-23. https://doi.org/10.9734/BJMCS/2016/27737
29. Tyagi AK, Kumari S, Fernandez TF, Aravindan C. P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. *et al*. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science; c2020. p. 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56
30. Amit Kumar Tyagi, Sreenath Niladhuri, ISPAS: An Intelligent, Smart Parking Allotment System for Travelling Vehicles in Urban Areas, International Journal of Security and Its Applications. 2017;11(12):45-66. ISSN: 1738-9976 IJSIA, SERSC Australia.
31. Nair Meghna Manoj, Tyagi Amit Kumar. Privacy: History, Statistics, Policy, Laws, Preservation and Threat Analysis, Journal of Information Assurance & Security. 2021;16(1):24-34.
32. Sravanthi K Burugari, Vijay Kumar, Tyagi Amit. Preserving Privacy Techniques for Autonomous Vehicles. 2020;8:5180-5190. 10.30534/ijeter/2020/48892020.
33. Mohan Krishna A, Amit Kumar Tyagi, Prasad SVAV. Preserving Privacy in Future Vehicles of Tomorrow, JCR. 2020;7(19):6675-6684. Doi: 10.31838/jcr.07.19.768
34. Amit Kumar Tyagi, Sreenath N. Preserving Location Privacy in Location Based Services against Sybil Attacks, International Journal of Security and Its Applications (ISSN: 1738-9976 (Print), ISSN: 2207-9629 (Online)). 2015 December 9;12:189-210.
35. Amit Kumar Tyagi, Sreenath N. A Comparative Study on Privacy Preserving Techniques for Location Based Services, British Journal of Mathematics and Computer Science (ISSN: 2231-0851). 2015 July;10(4):1-25.
36. Amit Kumar Tyagi, Sreenath N. Location Privacy

Preserving Techniques for Location Based Services over Road Networks, 2-4 April, in proceeding of IEEE/ International Conference on Communication and Signal Processing (ICCSP), ISBN: 978-1-4799-8080-2, Tamilnadu, India; c2015. p. 1319-1326.
37. Krishna M, Tyagi AK. Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE); c2020. p. 1-8. Doi: 10.1109/ic-ETITE47903.2020.332.
38. Amit Kumar Tyagi, Sreenath N. Vehicular Ad Hoc Networks: New Challenges in Carpooling and Parking Services, in proceeding of International Conference on Computational Intelligence and Communication (CIC), International Journal of Computer Science and Information Security (IJCSIS), Pondicherry, India. 2016;14:13-24.
39. Varsha R, *et al*. Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles. International Journal of Hybrid Intelligent System. 2020;16(4):223-236.
40. Amit Kumar Tyagi, Aswathy SU. Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks. 2021;2:83-102. ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.
41. Agrawal D, Bansal R, Fernandez TF, Tyagi AK. Blockchain Integrated Machine Learning for Training Autonomous Cars. In: *et al*. Hybrid Intelligent Systems. HIS 2021. Lecture Notes in Networks and Systems; c2022. p. 420. Springer, Cham. https://doi.org/10.1007/978-3-030-96305-7_4
42. Deekshetha HR, Shreyas Madhav AV, Tyagi AK. Traffic Prediction Using Machine Learning. In: Suma, V., Fernando, X., Du, KL., Wang, H. (eds) Evolutionary Computing and Mobile Sustainable Networks. Lecture Notes on Data Engineering and Communications Technologies; c2022. p. 116. Springer, Singapore. https://doi.org/10.1007/978-981-16-9605-3_68
43. Tyagi AK, Agarwal D, Sreenath N. SecVT: Securing the Vehicles of Tomorrow using Blockchain Technology, 2022 International Conference on Computer Communication and Informatics (ICCCI); c2022. p. 1-6. Doi: 10.1109/ICCCI54379.2022.9740965.
44. KV Tyagi AK, Kumar SP. Blockchain Technology for Securing Internet of Vehicle: Issues and Challenges, 2022 International Conference on Computer Communication and Informatics (ICCCI); c2022. p. 1-6. Doi: 10.1109/ICCCI54379.2022.9740856.
45. Amit Kumar Tyagi, Dr. N Sreenath. Providing Safe, Secure and Trusted Communication among Vehicular Ad-hoc Networks' Users: A Vision Paper, International Journal of Information Technology and Electrical Engineering. 2016;5(1):35-44.