Rajkumar,INDIA / International of Journal of Research and Computational Technology
Vol.14 Issue.3 Free Journal Publications pages:01-09
ISSN: 0975-5662 August,2022 www.ijrct.com

Internet of Things (IoT) Applications and Security Challenges

#Kandikonda.Rajkumar,Dept of Informatics,Email:kandikondarajkumar1@gmail.com

Abstract:

The internet of things (IoT) revolutionized the global community comprising of people, clever devices, sensible gadgets, information, and facts. It is no mystery that as increasingly devices connect with the internet, the challenges of securing the data that they transmit and the communications that they initiate have become more profound. Over time, we have seen a surge in IoT gadgets, widely in 2 regions – in homes and in production. With the former, we've got visible a whole environment built around Amazon's Echo devices the usage of the Alexa Voice provider. Google, Microsoft, and Apple have observed in shape as nicely. Due to the fact that these are impartial and closed systems, the responsibilities of securing the devices relaxation with the platform vendors. In this paper, we highlights cyber safety in manufacturing and associated industries. Industries along with manufacturing, oil & gas, refining, prescribed drugs, meals & beverage, water treatment, and lots of extra are constantly looking to add the proper layers of security, as they convey increasingly more device and gadgets on line. Tool manufacturers and plant operations managers continuously face strain to shield their bodily assets from cyber threats. Moreover, for each of those industries, the character of the data, topologies of IoT gadgets, and complexities of risk control and making sure compliance range extensively.

Keywords: Internet of Things, Cyber-attack, Security threats.

INTRODUCTION

The current rapid improvement of the internet of factors (IoT) and its capacity to offer one of a kind sorts of offerings have made it the fastest growing era, with large effect on social existence and business environments. Internet of factors (IoT) devices are swiftly becoming ubiquitous whilst IoT offerings have become pervasive. Their achievement has not long gone overlooked and the number of threats and assaults towards IoT gadgets and services are at the boom as well.

The internet of factors (IoT) is an idea that could extensively regulate our relationship with technology. The promise of a global in which all of the digital devices round us are a part of a single, interconnected network become once a factor of technological know-how fiction. But IoT has not handiest entered the arena of nonfiction; it's taking the sector by typhoon. IoT devices are no longer a gap market.

They have got started out to move from our workspaces into our (clever) homes, in which IoT devices are predicted to have the maximum sizable effect on our every day lives. Maximum clever home gadgets could be benign, normal home equipment like kettles and toasters. Even supposing those gadgets are hacked and compromised, brief of ruining yourbreakfast, there's no longer loads a hacker can do to purpose you grief. The market is currently focusing on the vertical domain names of IoT on the grounds that it's far in incredibly early levels of improvement. However IoT can't be dealt with as a single thing, or single platform, or maybe a unmarried era. So that it will attain the predicted speedy increase from IoT opportunities, extra awareness wishes to be placed on interfaces, platforms, cellular applications and not unusual/dominant standards [1][2].

IoT within the schooling quarter has already began to make the traditional education device more automated interactive smart lecture rooms are assisting

college students analyze and take part extra, whilst computerized attendance and diverse student monitoring systems should assist to make colleges greater secure. Net-enabled far flung lecture rooms can be a milestone for growing countries, making deep penetration in areas in which putting in place a conventional school infrastructure isn't always feasible.Internet-enabled manufacturing and business devices are giving differentiating outcomes, making them safer and extra green thru automatic manner controls. Plant and energy optimization, health and protection manipulate and protection control are now increasingly more being supplied via superior sensors, networked with sophisticated microcomputers [3][4].

Financial services are already leveraging the net for many of their services. Exponential development in virtual infrastructure and the next generation of IoT enabled merchandise ought to in addition lead the increase of the monetary area, with innovations, together with smart wearable and smart tracking devices, assisting clients to keep better tune in their money and investments. Telcos ought to face a surge in facts usage because of IoT-enabled gadgets, as a result elevating their ARPU (average sales in keeping with user), whilst then again, they may additionally ought to deal with some concerns, such as privacy and infrastructure security. While the possibilities of those new technology are thoughts-boggling, in addition they monitor intense IoT cybersecurity challenges. At some stage in the previous couple of years, we've seen a dramatic increase within the quantity and the sophistication of attacks targeting IoT devices.

The interconnectivity of people, devices and organizations in today's digital world, opens up a whole new playing field of vulnerabilities — access points where the cyber criminals can get in.

The overall risk "landscape" of the organization is only a part of a potentially contradictory and opaque universe of actual and potential threats that all too often come from completely unexpected and unforeseen threat actors, which can have an escalating effect. In this paper discussed various security challenges in IOT. The main contribution of this paper is to provide an overview of the current state of IoT security challenges [5].

INTERNET OF THINGS (IOT)

The net of factors, or IoT, is a machine of interrelated computing gadgets, mechanical and virtual machines, gadgets, animals or human beings that are provided with unique identifiers (UIDs) and the ability to transfer facts over a network with out requiring human-to-human or human-to- pc interplay A thing inside the internet of factors can be someone with a coronary heart display implant, a farm animal with a biochip transponder, an car that has constructed- in sensors to alert the motive force while tire pressure is low or any other natural or man-made object that can be assigned an IP deal with and is able to transfer facts over a community[6][7].

Increasingly more, organizations in a spread of industries are the use of IoT to function greater efficaciously, higher apprehend customers to deliver more advantageous customer support, enhance decision-making and boom the price of the enterprise [8].The net of factors (IoT) is a computing idea that describes the idea of everyday physical gadgets being related to the internet and being able to pick out themselves to other devices. [9]

The term is closely diagnosed with RFID as the technique of communication, even though it additionally may additionally include different sensor technologies, wireless technologies or QR codes.

CHARACTERISTICS OF INTERNET OF THINGS (IOT)

Some most popular characteristics of Internet of things are:

(a) Intelligence
(b) Connectivity
(c) Dynamic Nature
(d) Enormous scale
(e) Sensing
(f) Heterogeneity
(g) Security

(a) Intelligence

IoT comes with the aggregate of algorithms and computation, software & hardware that makes it clever. Ambient intelligence in IoT complements its abilities which facilitate the things to respond in an clever manner to a particular scenario and helps them in carrying out unique tasks. In spite of all the popularity of smart technology, intelligence in IoT is only concerned as manner of interplay between devices, whilst user and tool interaction is achieved by using general input strategies and graphical user interface [8].

Together algorithms and compute (i.E. Softwaren & hardware) provide the "smart spark" that makes a product revel in clever. Bear in mind Misfit Shine, a fitness tracker, compared to Nest's smart thermostat. The Shine experience distributes compute obligations between a smartphone and the cloud. The Nest thermostat has greater compute horsepower for the AI that lead them to clever.

(b) Connectivity

Connectivity empowers internet of factors via bringing collectively everyday items. Connectivity of those items is pivotal due to the fact easy item stage interactions make a contribution in the direction of collective intelligence in IoT community. It allows network accessibility and compatibility within the things. With this connectivity, new market possibilities for net of factors can be created by way of the networking of clever things and applications.

Connectivity within the IoT is extra than slapping on a WiFi module and calling it an afternoon. Connectivity permits community accessibility and compatibility. Accessibility is getting on a network while compatibility offers the commonplace ability to eat and convey facts. If this sounds familiar, that's because it's miles Metcalfe's law and it rings genuine for IoT [10].

(c) Dynamic Nature

The primary activity of internet of things is to acquire records from its environment, that is executed with the dynamic modifications that take vicinity across the gadgets. The state of those gadgets trade dynamically, instance napping and waking up, related and/or disconnected as well as the context of devices which include temperature, region and pace. Further to the state of the tool, the quantity of gadgets additionally changes dynamically with a person, place and time.The kingdom of gadgets trade dynamically, e.G., sleeping and waking up, linked and/or disconnected in addition to the context of gadgets which include location and velocity. Moreover, the variety of devices can change dynamically [11].

(d) Enormous scale

The quantity of gadgets that want to be controlled and that communicate with every different might be a great deal larger than the devices connected to the contemporary internet. The control of statistics generated from these gadgets and their interpretation for utility functions will become more vital. Gartner (2015) confirms the giant scale of IoT within the envisioned record in which it stated that 5.5 million new things gets related every day and six.Four billion related matters will be in use global in 2016, which is up through 30 percentage from 2015. The report also forecasts that the number of linked gadgets will attain 20.8 billion through 2020.The number of devices that want to be controlled and that communicate with each other can be at least an order of importance large than the gadgets linked to the current internet. Even more critical may be the control of the information generated and their interpretation for software purposes. This relates to semantics of information, in addition to green statistics managing.

(e) Sensing

IoT wouldn't be feasible with out sensors as a way to hit upon or measure any modifications in the surroundings to generate statistics that may file on their fame or even interact with the environment. Sensing technology offer the method to create competencies that reflect a true focus of the physical international and the people in it. The sensing statistics is certainly the analogue input from the bodily international, however it is able to offer the wealthy know-how of our complicated world [12] [13].We generally tend to take as a right our senses and ability to apprehend the bodily world and people round us. Sensing technologies offer us with the manner to create experiences that replicate a real focus of the bodily global and the human beings in it. This is genuinely the analog enter from the bodily global, however it is able to provide wealthy information of our complex international.

(f) Heterogeneity

Heterogeneity in net of factors as one of the key traits. Devices in IoT are based on specific hardware structures and networks and can interact with other gadgets or carrier systems through distinctive networks. IoT structure have to support direct network connectivity among heterogeneous networks. The important thing design necessities for heterogeneous things and their environments in IoT are scalabilities, modularity, extensibility and interoperability. The devices within the IoT are heterogeneous as based totally on distinct hardware platforms and networks. They are able to interact with different gadgets or provider systems via unique networks [14].

(g) Security

IoT devices are clearly at risk of security threats. As we benefit efficiencies, novel experiences, and different benefits from the IoT, it would be a mistake to forget about approximately safety worries associated with it. There may be a excessive degree of transparency and privacy problems with IoT. It is vital to secure the endpoints, the networks, and the data this is transferred across all of it way developing a security paradigm.

APPLICATIONS OF INTERNET OF THING (IOT)

Some useful applications of Internet of Things (IOT) are:

(a) Connected Health
(b) Smart City
(c) Connected Cars
(d) Smart Home
(e) Smart Farming
(f) Smart Retail
(g) Smart Supply Chain

(a) Connected Health (Digital Health/Tele health/Telemedicine)

IoT has various applications in healthcare, which are from remote monitoring equipment to advance & smart sensors to equipment integration. It has the potential to improve how physicians deliver care and also keep patients safe and healthy. Healthcare IoT can allow patients to spend more time interacting with their doctors by which it can boost patient engagement and satisfaction. From personal fitness sensors to surgical robots, IoT in healthcare brings new tools updated with the latest technology in the ecosystem that helps in developing better healthcare. IoT helps in revolutionizing healthcare and provides pocket-friendly solutions for the patient and healthcare professional [15][16].

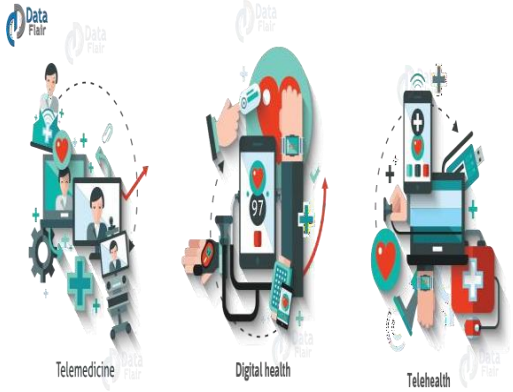

Figure 1: Connected Health

Connected healthcare yet remains the sleeping giant of the Internet of Things applications. The concept of connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness. The video below explains how IoT can revolutionize treatment and medical help.

(b) Smart City

Smart metropolis is some other effective application of IoT producing curiosity amongst international's populace. Smart surveillance, smarter power control systems, automatic transportation, water distribution, city safety and environmental tracking all are examples of net of factors programs for clever towns. IoT will solve most important issues faced by the humans living in towns like pollution, visitors congestion and lack of energy supplies and many others. Merchandise like cell conversation enabled clever stomach trash will ship signals to municipal services whilst a bin needs to be emptied [17].

Figure 2: Smart City

With the aid of putting in sensors and using internet programs, citizens can locate loose available parking slots throughout the town. Additionally, the sensors can discover meter tampering issues, popular malfunctions and any installation problems in the electricity gadget.

(c) Connected Cars

The car virtual era has targeted on optimizing motors inner functions. However now, this interest is developing toward improving the in-automobile enjoy. A linked car is a vehicle which is capable of optimize its personal operation, maintenance in addition to comfort of passengers the use of onboard sensors and net connectivity. Most huge automobile makers in addition to a few courageous startups are operating on connected car answers. Foremost brands like Tesla, BMW, Apple, and Google are working on bringing the following revolution in motors [18]

.

Figure 3: Connected Cars

Connected car generation is a tremendous and an intensive community of a couple of sensors, antennas, embedded software, and technologies that assist in conversation to navigate in our complex global. It has the responsibility of creating decisions with consistency, accuracy, and speed. It also needs to be reliable. Those requirements will become even extra essential when humans surrender totally the manage of the steering wheel and brakes to the self reliant or automated motors that are being effectively tested on our highways proper now.

(d) Smart Home

Clever domestic has come to be the innovative ladder of fulfillment inside the residential spaces and it's miles predicted smart houses will become as common as smartphones each time we consider IoT systems, the most vital and efficient software that stands out on every occasion is wise home ranking as highest IOT utility on all channels. The estimated amount of funding for clever home startups exceeds $2.5bn and is ever growing. Wouldn't you love if you may turn on air con before achieving home or transfer off lighting fixtures even after you've got left domestic? Or free up the doors to buddies for brief get right of entry to even whilst you aren't at home. Don't be surprised with IoT taking form groups are building products to make your lifestyles less complicated and convenient [11].

The fee of owning a house is the most important fee in a homeowner's existence. Clever home products are promised to store time, strength and cash. With clever home agencies like Nest, Ecobee, Ring and August, to name some, will become family brands and are planning to supply a by no means seen earlier than enjoy [19].

Figure 4: Smart Home

(e) Smart Farming

Clever farming is an frequently disregarded IoT utility. However, due to the fact the variety of farming operations is usually far flung and the massive wide variety of cattle that farmers paintings on, all of this can be monitored by way of the net of factors and can also revolutionize the way farmers work. However this concept is yet to attain a huge-scale attention. Though, it still remains to be one of the IoT programs that have to not be underestimated. Clever farming has the potential to grow to be an crucial utility field mainly within the agricultural-product exporting countries.

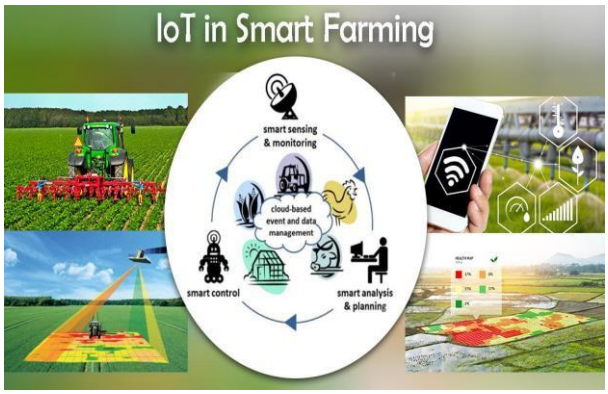

Figure 5: Smart Farming

(f) Smart Retail

Outlets have started adopting IoT solutions and using IoT embedded systems throughout a number of programs that enhance keep operations consisting of increasing purchases, lowering robbery, allowing inventory management, and enhancing the purchaser's buying revel in. Through IoT physical stores can compete against on line challengers greater strongly.

They can regain their lost marketplace proportion and appeal to consumers into the store, consequently making it less complicated for them to shop for extra at the same time as saving cash [20].

Figure 6: Smart Farming

Deliver chains have already been getting smarter for more than one years. Imparting solutions to troubles like tracking of products whilst they may be on the road or in transit, or supporting providers change inventory records are a number of the famous services. With an IoT enabled machine,manufacturing facility device that includes embedded sensors speak information about one-of-a-kind parameters which incorporates pressure, temperature, and usage of the device. The IoT system also can manner workflow and exchange device settings to optimize general performance [21].

(g) Smart Supply Chain

Supply chains have already been getting smarter for multiple years. Imparting answers to troubles like monitoring of products while they are on the street or in transit, or assisting suppliers alternate stock records are a number of the famous services. With an IoT enabled gadget,manufacturing facility gadget that includes embedded sensors speak information approximately one-of-a-kind parameters which includes strain, temperature, and usage of the machine. The IoT system also can manner workflow and change system settings to optimize overall performance [21].

Figure 7: Smart Supply Chain

SECURITY CHALLENGES FACING IOT:

IoT protection is the protection of net of things gadgets from attack. At the same time as many commercial enterprise proprietors are aware that they need to defend computer systems and phones with antivirus, the safety risks related to IoT devices are much less widely recognized and their protection is simply too frequently not noted.Internet of things gadgets are anywhere. From motors and refrigerators to monitoring devices on assembly strains, objects around us are more and more being linked to the net.

The speed at which the IoT marketplace is growing is mind-blowing- Juniper studies estimates that the variety of IoT sensors and devices is ready to exceed 50 billion through 2022.At the same time as customer IoT gadgets allow lifestyle blessings, businesses are fast adopting IoT gadgets because of excessive capacity for savings. For instance, after Harley-Davidson turned their York, Pennsylvania plant to a 'clever manufacturing facility' using IoT gadgets in each step of the manufacturing method, they decreased fees by 7% and multiplied internet margin by means of 19%.

(a) Data Integrity

Billions of gadgets come under the umbrella of an interlinked surroundings that is related thru IoT. Manipulating even a single records point will bring about manipulation of the entire facts that's exchanged and shared from side to side from the sensor to the main server. Decentralized disbursed ledger and digital signatures ought to be implemented that allows you to make certain integrity [24].

(b) Encryption Capabilities

Data encryption and decryption is a continuous process. The IoT network's sensors still lack the capability to process. The brute force attempts can be prevented by firewalls and segregating the devices into separate networks.

(c) Privacy Issues

IoT is all about the exchange of data among various platforms, devices, and consumers. The smart devices gather data for a number of reasons, like, improving efficiency and experience, decision making, providing better service, etc.; thus, the end point of data shall be completely secured and safeguarded.

(d) Common Framework

There is an absence of a common framework and so all the manufacturers have to manage the security and retain the privacy on their own. Once a common standardized framework is implemented, the individual efforts will then collectively be utilized in an expandable manner and so reusability of code can be achieved [23].

(e) Automation

Eventually, enterprises will have to deal with more and more number of IoT devices. This enormous amount of user data can be difficult to manage. The fact cannot be denied that it requires a single error or trespassing a single algorithm to bring down the entire infrastructure of the data [22].

(f) Updations

Managing the update of millions of devices needs to be adhered to, respectively. Not all the devices guide over the air update and for this reason it calls for manually updating the devices. One will want to keep a track of the to be had updates and follow the identical to all of the varied devices. This technique becomes time-ingesting and complex and if any mistake occurs in the system than this shall cause loopholes inside the protection later. Security investment in securing infrastructure and community must be the first priority, which isn't the case now. IoT entails the use of thousands and thousands of facts points and every factor ought to be secured. Indeed, the need is for the multi-layer safety, i.E., security at every and every degree. From end-point gadgets, cloud systems, embedded software program to web and mobile programs that leverage IoT (internet of things), every layer have to be security intact. With the set of heterogeneous devices, protection will become complicated.

Figure 8: Security Vhallenges Facing IOT

CONCLUSION

The IoT framework is prone to attacks at every layer. Consequently, there are numerous safety threats and requirements that want to be dispatched. Modern-day kingdom of research in IoT is mainly focused on authentication and get entry to manage protocols, but with the rapid increase of technology it's far vital to consolidate new networking protocols like IPv6 and 5G to acquire the revolutionary mash up of IoT topology the primary emphasis of this bankruptcy become to focus on fundamental security problems of IoT specifically, focusing the security assaults and their countermeasures. Due to lack of safety mechanism in IoT gadgets, many IoT gadgets end up soft targets and even this is not inside the victim's know-how of being inflamed. In this chapter, the safety necessities are mentioned such as confidentiality, integrity, and authentication, and so on. In this paper, different programs of IOT are mentioned. We hope this paper can be beneficial to researchers within the security discipline by using supporting discover the principal issues in IoT protection and offering better understanding of the threats and their attributes originating from various intruders like companies and intelligence companies.Final and now not published in any conferences or in any journal.

REFERENCES

[1] R.Vignesh and 2A.Samydurai ans1 Student, 2Associate Professor Security on Internet of Things (IOT) with Challenges and Countermeasures in 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.

[2] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.

[3] J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.

[4] Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.

[5] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.

[6] M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5,86-97, 2012.

[7] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.

[8] Mirza Abdur Razzaq and Muhammad Ali Qureshi "Security Issues in the Internet of Things (IoT): A Comprehensive Study" by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[9] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.

[10] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[11] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with chinaperspective,"IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[12] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"Comput. Netw. vol. 54, no. 15, pp. 2787–2805, Oct 2010.

[13] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey,"IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[14] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santana, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.

[15] A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014,pp. 372–374.

[16] Mohamed Abomhara and Geir M. Køien" Cyber Security and the Internet of Things:

Vulnerabilities, Threats, Intruders and Attacks".

[17] S. De, P. Barnaghi, M. Bauer, and S. Meissner, "Service modelling for the internet of things," in Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, 2011, pp. 949–955.

[18] G. Xiao, J. Guo, L. Xu, and Z. Gong, "User interoperability with heterogeneous iot devices through transformation," 2014.

[19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions, "Future Generation Computer Systems, vol. 29, no. 7,pp. 1645–1660, 2013.

[20] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view," Wireless Communications, IEEE, vol. 17, no. 6, pp. 44–51,2010.

[21] C. Hong song, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on. IEEE, 2011, pp. 286–290.

[22] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2 communication," Vehicular Technology Magazine, IEEE, vol. 4,no. 3, pp. 69–75, 2009.

[23] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks.