International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Major Challenges and Concerns of Internet of Things (Iot) Security in Critical Healthcare

Raghu Ram Nallani Chakravartula, V. Naga Lakshmi

Abstract: ***In an IoT space, everyday objects are equipped with microprocessors for data acquisition, transceivers to enable them to sense the surroundings and transfer with each other over the Internet. In this environment, intelligent objects can communicate with one another forming a promising model to offer services that can be accessible to anyone, anywhere, anytime. It has been widely accepted that our daily lives will be fundamentally enriched with various IoT services in healthcare domain. The inherent nature of the Internet of Things technology makes it an indispensable choice for patient monitoring in critical care areas. Along with the incredible opportunities provided by IoT, it also opens new risks and threats. As more and more medical devices are interconnected, they are increasingly exposed to security risks, malware, and user's privacy. The rise in new attack vectors and poorly configured device settings may become a potential target for hackers to compromise affecting the resilience of the medical devices Hackers & targeted attacks could not only impair the medical devices functionality but potentially adversely effect on patient safety. The paper presents on the impact of security across IoT objects. and discusses how authentication, authorization, availability, confidentiality, integrity, and non-repudiation and privacy plays a critical role in the success of IoT.***

Keywords**:** ***Internet of things, Security, Privacy, Critical Healthcare, Challenges and concerns.***

I. INTRODUCTION

The "IoT is considered as the 3rd wave of connectivity" in Internet space. More than one billion hosts are connected in the early 1990's in its first phase. Mobile is regarded as the second wave where another 2 billion devices are connected in the 2000's. It's assumed "to associate 10x as many objects by 2020" [1]. Predictions, projections depict the importance of IoT and shows the technology a game changer. On the other hand, Security and privacy aspects are considered as a crucial differentiator to embrace the Internet of Things in the healthcare domain. 48 percent of U.S. companies using the Internet of Things have suffered security breaches due to the lack of enough controls for security and privacy. The recent survey from Alman Vilandrie and company revealed that the cost of those breaches ranged from hundreds to millions of dollars [2].

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Raghu Ram Nallani Chakravartula*, Research Scholar, GITAM university, Visakhapatnam, Andhra Pradesh, India.
V. Naga Lakshmi, Heading the Department of computer science in GITAM, Visakhapatnam, Andhra Pradesh, India.

Hewlett Packard study shows that 80% of the smart objects had inadequate Authorization and Authentication controls [3]. Recent media reports back up the above findings with significant vulnerabilities growing daily.

II. SIGNIFICANCE OF IOT

The predictions and projections made on IoT by prominent research and technology firms depicts the importance of IoT and its applications. In 2011, Cisco forecasted that "by the year 2020, 50 billion connected devices would exist which would be more than 40 times to that of the human population thereby generating 14.4 trillion of value over the next decade" [4].

Ericsson figures on an estimate of "around 28 billion number of devices being connected by 2021 [5] and IDC anticipates 28.1 billion in the same time" [6]. In 2012, IBM predicted there would be "one trillion devices connected in a decade" [7]. IHS Markit estimates "30.7 billion IoT devices for 2020 and the same is estimated to increase by 125 Billion by 2030" [8].

Gartner, Inc. expects "the number of connected things would reach 20.8 billion by 2020 and determines that the total services spending will reach an estimate of $1,534 billion and $1477 in consumer applications and enterprise applications respectively" [9]. E & Y research shows that "IoT provides enhanced customer experience and drives exponential revenue" [10].

As per PWC, "$6 trillion will be spent on IoT-based solution and services between the years 2015 – 2020" [11]. Forbes predicted that "the IoT market globally would increase to $457 billion by the year 2020, with a CAGR of 28.5%" [12]. Bain forecasts "Business-to-Business (B2B) market will generate more than $300 billion annually by 2020" [13].

Boston Consulting Group (BCG) predicts that "the IoT Market to would reach $267 billion by the year 2020." [14].

Verizon study on IoT adoption finds "massive growth in all domains and manufacturing was leading" [15].

McKinsey Global Institute estimates that "IoT could become an economic influencer of a value of $11.1 trillion by 2025." [16]. Statista forecasts that "the installed IoT devices base would increase worldwide by a value of 31 billion by the year 2020" [17]. The cognizant study reveals that "companies shall expand their expenses on IoT by 72% in next 3 years." [18].

IoTelecom study shows that "global market is forecasted to increase $661.74 Billion by 2021" [19]. Accenture estimates the "IoT could generate an estimate of $14.2 Trillion to the economy by 2020" [20].

IoT Security attracted interest of academic, research, industry communities equally.

The same has been illustrated using Google trends between the years 2004 to 2018 as shown in below figure 1. [21].

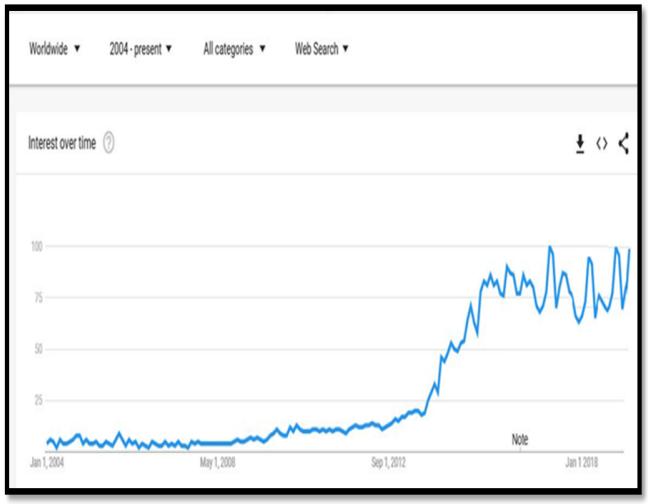

Figure 1 IoT Security in Google Trends between the years 2004 to 2020 (present)

The number of research publications in IEEE journals, conferences, and magazines on IoT security is captured in figure 2 below [22]

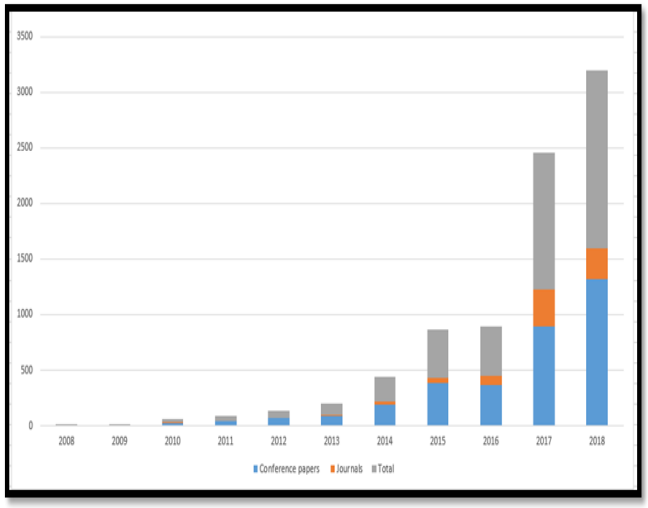

Figure 2 IEEE Technical publications on IoT Security from the year 2008 to 2020 (Present)

III. APPLICATIONS OF IOT

Internet of Things is going to be the next game changer that ensure to transform the way we learn, work, play and live. Internet of Things may redefine social, economic and technical elements in many sectors with accelerated growth resulting in innovative and novel applications. The large-scale implementation of IoT devices brings tremendous opportunity with disruptive applications as depicted in the below figure 3. [23]

A. Agriculture and Farming

The world population is set to touch 11.2 billion in 2100 according to united nation DESA report on "world population prospects in 2015 revision". With traditional farming approaches, it will not be possible to meet the needs of the massive population across the world. On the other hand, extreme climatic conditions like rainfall, humidity, heat will affect the yield of crops. Also, there is much focus on improving the production of organic crops without using pesticides and artificial chemical manures.

Agriculture and farming industry started embracing the Internet of things to handle the above challenges and demands. In IoT farming allows to track, govern and forecast the crop fields with the aid of sensors for improved productivity. Some of the critical areas of research include the use of drones and vehicle monitoring, support for precision farming, livestock monitoring, and smart greenhouses.

B. Banking and Finance sector

The adoption of IoT in the banking and finance sectors helps drastically in the reduction of fraudulent transactions, faster payments, reduction of charges, and improved operability by supporting blockchain smart contracts to decentralize the operations.

C. Consumer electronics and utilities

Several Consumer electronics objects are already connected to the Internet. Some of the examples are intelligent toothbrushes, energy-saving lights, fans and refrigerators, Smart televisions.

D. Automotive transportation

According to a Bernstein report, the total vehicle count globally will nearly double, the air travel or the kilometers flown in planes is expected to cross 20 trillion by 2040. With such massive growth, there would be growth in traffic congestion, traffic accidents, parking, fuel consumption, and pollution concerns. IoT shall alter and revolutionize industry with self-driving cars, smart fleet management with intelligent tracking and routing management, driver behavior monitoring and vehicle performance, environment monitoring, prevention of theft, smart toll collection, automatic braking in railways, collision control, smart parking, better flow control are few to name. It ensures logistics in delivering the product to the right place, time, to the intended party in excellent condition with minimal human intervention.

E. Environmental

According to the Scientific American study, it proved that Deforestation accounts for 15% of all global warming by emitting carbon dioxide. Internet of things to address different aspects of conservation like the prevention of deforestation and poaching, preservation of biodiversity and data collection. Increased efficacy and efficiency in smart homes and smart cities will help us conserve energy, water, and natural resources will have a significant impact on the Environment.

F. Smart cities

It is estimated that more than 50% of the population all across the globe is moving to urban areas and cities. It puts much focus on sustainable living, and it affects various domains like infrastructure, environment, and transportation.A smart city uses digital technologies and data collected to improve the lives of its citizens. IoT based Smart cities helps to transform cities by optimizing natural resources usage and greener energy transmission, It helps to reduce the operational costs, make emergency system more efficient by creating safer cities, it creates efficient servicing and optimizing the cost,

it increases satisfaction to end users, It makes a positive impact with greater transparency and productivity. It offers new enhanced services in the domains of oil, gas, water, mining, forestry, energy domains.

G. Industry and automation

The Primary challenge in the manufacturing industry is to deliver high-quality products at a competitive price. To address the above challenge,
Industry must embrace the Internet of things to automate devices, increase reliability and quality of the product, by designing cost involved in design or production by adopting integrating and innovative services. The Internet of things is disrupting several industrial systems like Human-Machine Interface (HMI), Enterprise Asset Management (EAM), Machine Safety Systems (MSS), Supervisory Control and Data Acquisition system (SCADA), General Motion Control (GMC), Operator Training Simulators (OTS), sensors and transmitters, Distributed Control System (DCS) in across several industries such as oil, power and gas, chemicals and petrochemicals, defense, and automotive, food and beverage and aerospace, etc.

H. Health and well-being

As per the estimates, majority of the world's population above 60 years of age shall reside in the developing countries. Conventional medical processes and devices will not sustain the growing needs of an elderly population. As life expectancy rises, the cost of health care will increase exponentially.
Integrating IoT features into health care improves the quality of service with the improvement in patient outcomes, lower costs, and create efficiencies. It enables remote monitoring, wearable sensors and reduces readmissions by providing proactive care; It accelerates precision and predictive medicine with data collected from various devices.

I. Utilities

The use of Internet of things in utility sector helps to meet the demands by an increase in production, prevent failures and outages, provide operational efficiency thereby decreasing the cost using automation, improve and manage asset health and enhance end-user experience, Major utility sector comprises of Energy, gas, water, oil.

IV. CHALLENGES AND CONCERNS OF IOT

It has been widely accepted that our daily lives will be fundamentally enriched with various IoT services across sectors. Along with the incredible opportunities provided by IoT, it also opens new risks and threats. These include user privacy, security, standards & interoperability, compliance, legal & regulatory, and emerging economies and development as illustrated in figure 8. [24]

A. Security

IoT is an interconnected grid of smart objects. In such a network, authentication, authorization, availability, confidentiality and integrity plays a critical role. The rise in new attack vectors and poorly configured device settings may become a potential target for hackers to compromise affecting the resilience of the Internet. [25, 26, 27].

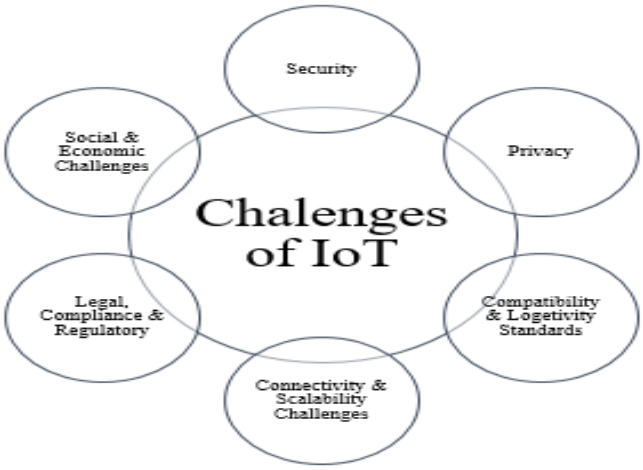

Figure 3 Challenges of the Internet of Things (IoT)

B. Privacy

As the objects, people and their environment become tightly intertwined, sensitive data has been collected, analyzed, stored and communicated across the network to avail respective services. In such a network, respecting user's privacy choices is another critical area to reveal the full potential of the IoT services. [28,29].

C. Compatibility, Interoperability and Longevity Challenges

Due to the high amount of proliferation of heterogeneous objects in IoT and due to lack of international mutually agreed compatibility standards across IoT vendors lead to vendor lock-in, inflexibility in integration with other components and modules. Also, the possibility of many of these technologies becoming obsolete shortly and the devices tend to be functioning with no vendor service, or support leads to an increase in ownership complexity [30].

D. Connectivity and Scalability Challenges

Networking protocols designed in the early 1970's will not be able to support millions of smarter objects connecting and interacting over the Internet. As IoT is still in its infancy today and newer protocols should be designed to support a broad stream of implementation. [31]

E. Legal, Compliance, and Regulatory

Innovative IoT-based applications promote novel models to speak, trust connect, share, innovate, and choose. These newer models pose a new set of legal, compliance and regulatory challenges regarding data retention & destruction, security breach and unintended usage of applications, lapses with privacy, cross-border data sharing & storage issues, etc. Existing standards will not suffice and a newer set of legal. Compliance and regulatory standards need to be formulated to address the above.

F. Emerging social, economies and development challenges

Delivering social and economic benefits to developing and emerging societies possess several implementation challenges like readiness in the underlying infrastructure, Government support for investment incentives, fulfillment of technical skills shortage, formulating legal laws and policies to support the newer development, etc.
[32]

V. PATIENT HEALTH MONITORING IN CRITICAL HEALTHCARE

To achieve the best possible outcomes in the patient's health condition, monitoring of critical parameters is essential [33, 34]. Monitoring may occur on an intermittent basis, such as having the blood pressure checked during an annual physical examination or in a continuous manner such as monitoring breathing when anesthetized during an operation. Internet of Things plays pivotal role in patient diagnosis, monitoring and their treatment. [35]. Parameters are merely the measurements of vital bodily functions. The determination of which parameters to monitor varies by patient condition. In some cases, the monitoring processes are painless and take seconds. Other parameters require invasive procedures to place tubes, sensors,

and probes within the heart, vessels, and lungs. Invasive procedures result in an increased risk of injury or infection for the patient and typically are more expensive. The objective is to compare the physiological data available to normal limits, to make emergent and long terms decisions in the care of the patient. Sometimes data points are taken into consideration in conjunction with other patient assessment data such as level of consciousness, pain, and the patient's past and current medical history to improve the patient's health. A drastic change in a parameter will generate an alarm and cause concern; fortunately, it does not always mean the patient's condition is deteriorating. The alarm signals the need to check on the patient. Patients have been known to remove electrodes or disconnect themselves from the monitoring devices when confused or agitated, to go for a walk or go to the bathroom. False alarms also occur. While universal levels of normal are already established, alarm limits (high and low), as well as alarm priorities, may vary from organization to organization [36]. The goal of medical facility is to enhance the patient's state of being or at minimum ease their suffering. Internet of things helps by providing solutions, which generate detailed patient information and make it readily available over the Internet to right stakeholders, necessary to make rapid and accurate decisions by the panel of doctors to achieve the best patient outcomes. The research is focused on securing IoT based medical devices used in life care support of patients in critical care areas.

VI. RESULT ANALYSIS OF CHALLENGES OF INTERNET OF THINGS (IOT) VS TRADITIONAL SYSTEMS

The following are the challenges in the traditional computing environment Vs the Internet of things (IoT) objects:

Analysis	Description
Infrastructure	Traditional computing is based on the client-server computing model; whereas most IoT-based devices are in ad-hoc. Thereby, any solutions which are designed for the traditional network devices won't be compatible with IoT objects.
Availability	The availability of source and destination nodes and connectivity between the source server and destination client is a challenge in IoT space.
Human interaction	Traditional systems would need human interaction to perform authentication and authorization like entering a password or by placing the finger as biometric information. IoT devices would expect minimal to no human intervention & most decisions would happen spontaneously.
Privacy	The IoT-based services collect user sensitive data to offer anytime anywhere services. Privacy of user's data poses a significant risk compared to traditional computing model.
Resource constraint nature of devices	Due to the limited power of the devices like processing, memory and bandwidth, the devices cannot process the cryptographic ciphers which are designed for traditional infrastructure. New cryptographic ciphers are required to accommodate the needs and requirements of the IoT objects.
Existing threats	Threats on availability to block denial of service (DoS) and Distributed Denial of Service (DDoS) is critical to ensure the devices are available. The existing infrastructure like firewall, Intrusion Detection System (IDS), Intrusion prevention System (IPS) are all based on signatures. The threats are blocked if and only if the existing signature is detected. These mechanisms won't be effective across IoT objects as the devices are limited and won't be able to accommodate above solutions.
Zero days and Targeted attacks	New threats and attack vectors in IoT based devices would bring new challenges. Also, targeted attacks on a specific device or vendor would pose significant risk to the devices.

VII. CONCLUSION

The paper provides solid introduction to the significance of Internet of thing and growing objects in day-to-day life in critical healthcare domain. In the medical healthcare sector, any accidental or deliberate security and privacy incidents of patient's information may not only cause monetary loss but also lead to embarrassment, societal pressures, and discrimination or may even kill a patient. Hence, any lapse in addressing security and privacy issues may face damage to reputation, lawsuits, embarrassment, and fines and bound by regulatory authorities. Due to large-scale implementations of IoT projects all over the globe and significant security findings, there is an immediate need to address its security risks and the paper provides foundation for the same.

ACKNOWLEDGMENT

The authors would like to thank General Electric Healthcare and Philips Healthcare support staff for helping us to measure, analyze patient healthcare monitoring sensors to experiment with various scenarios as part of the study.

REFERENCES

1. Internet of things infographics, web source, Retreived on Jan 9, 2020 from https://salesforce.com
2. Security Attacks on IoT, Web Source, Retrieved on Jan 9, 2020 from http://www.altvil.com/wp-content/uploads/2017/06/AVCo.-IoT-Security-White-Paper-June-2017.pdf
3. Hewlett Packard Internet of things infographics, web source, Retreived on Jan 9, 2020 from https://hp.com
4. Cognizant Digital Industrial Transformation with the Internet of Things, Web Source, Retreived on Jan 9, 2020 from https://www.cognizant.com/services-resources/Services/2017_pac_mcs_digital_industrial_iot_report.pdf
5. Ericsson Internet of things infographics, web source, Retreived on Jan 9, 2020 from https://ericson.com
6. IDC Infographics, Web Source, Retreived on Jan 9, 2020 from https://www.idc.com/infographics/IoT
7. IBM - An enterprise scale IoT Platform, Web Source, Retreived on Jan 9, 2020 from https://www.ibm.com/blogs/internet-of-things/enterprise-scale-iot-platform-watson/
8. IHS Markit press release, Web Source, Retreived on Jan 9, 2020 from https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
9. Gartner Infographics on Internet of things, Web Source, Retreived on Jan 9, 2020 from https://www.gartner.com/newsroom/id/3165317
10. E & Y: Internet of Things Human-machine interactions that unlock possibilities, Web source, Retrieved on Jan 9, 2020 from https://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/%24FILE/ey-m-e-internet-of-things.pdf
11. PWC Estimates on IoT, Web Source, Retreived on Jan 9, 2020 from https://www.pwc.fr/fr/assets/files/pdf/2017/03/2017_ai_and_iot_v13b.pdf
12. Forbes forecast on IoT, Web Source, Retreived on Jan 9, 2020 from http://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/
13. Bain forecast on IoT, Web Source, Retreived on Jan 9, 2020 from http://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/
14. Boston Consulting group: Technology notes on IoT, Web Source, Retreived on Jan 9, 2020 from https://www.bcg.com/industries/technology-industries/making-jump-to-internet-of-things.aspx
15. Verizon State of market: IoT, Web Source, Retreived on Jan 9, 2020 from http://www.verizon.com/about/sites/default/files/Verizon-2017-State-of-the-Market-IoT-Report.pdf
16. McKinsey: Whats new with the Internet of Things (IoT), Web Source, Retreived on Jan 9, 2020 from https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things
17. Statista: IoT Number of connected devices world wide, Web source, Retreived on Jan 9, 2020 from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
18. Cognizant Digital Industrial Transformation with the Internet of Things, Web Source, Retreived on Jan 9, 2020 from https://www.cognizant.com/services-resources/Services/2017_pac_mcs_digital_industrial_iot_report.pdf
19. IO Telecom: IoT Growth forecast, Web Source, Retreived on Jan 9, 2020 from https://www.slideshare.net/IQGroup/iot-growth-a-forecast
20. Accenture study on Industrial IoT, Web Source, Retreived on Jan 9, 2020 from https://www.slideshare.net/AugmentedWorldExpo/pete-wassell-augmate-ar-smart-glasses-and-the-industrial-iot
21. Google Trends, Web Source, Retrieved on Jan 9, 2020 from https://trends.google.com/trends/
22. IEEE Xplore Digital Library, Web Source, Retreived on Jan 9, 2020 from https://ieeexplore.ieee.org/
23. W. Meng, K. R. Choo, S. Furnell, A. V. Vasilakos and C. W. Probst, "Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 761-773, June 2018.
24. M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55
25. Y. Yang, H. Peng, L. Li and X. Niu, "General Theory of Security and a Study Case in the Internet of Things," in IEEE Internet of Things Journal, vol. 4, no. 2, pp. 592-600, April 2017.
26. S. L. Keoh, S. S. Kumar and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," in IEEE Internet of Things Journal, vol. 1, no. 3, pp. 265-275, June 2014.
27. Alasdair Gilchrist, IoT Security Issues, (2017)
28. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," in IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99-109, 1 April-June 2015.
29. S. Sharma, K. Chen and A. Sheth, "Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems," in IEEE Internet Computing, vol. 22, no. 2, pp. 42-51, Mar./Apr. 2018.
30. R. Giaffreda, L. Capra and F. Antonelli, "A pragmatic approach to solving IoT interoperability and security problems in an eHealth context," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 547-552, 2016
31. S. Pérez, J. A. Martínez, A. F. Skarmeta, M. Mateus, B. Almeida and P. Maló, "ARMOUR: Large-scale experiments for IoT security & trust," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 553-558.
32. V. A. F. Almeida, D. Doneda and M. Monteiro, "Governance Challenges for the Internet of Things," in IEEE Internet Computing, vol. 19, no. 4, pp. 56-59, July-Aug. 2015.
33. Jesse M. Ehrenfeld , Maxime Cannesson, Monitoring Technologies in Acute Care Environments: A Comprehensive Guide to Patient Monitoring Technology (2014)
34. J F Payne, J P Crul, Patient Monitoring (1970)
35. Jasvini R. Jayendran Pillai, Lee Yeng Seng, Nur Shazana Binti Abdul Rahman, Patient Monitoring System Using Cloud System And Arduino Atmega (2018)
36. Luis Ayala, Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention 1st ed. Edition, (2016)E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” IEEE Trans. Antennas Propagat., to be published.
37. J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” IEEE J. Quantum Electron., submitted for publication.
38. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
39. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces (Translation Journals style),” IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].
40. M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
41. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). Title (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
42. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com.
43. (Journal Online Sources style) K. Author. (year, month). Title. Journal [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL).

AUTHORS PROFILE

Raghu Ram Nallani Chakravartula is currently heading the information security and compliance in Mirra Healthcare, USA. He has 16+ years of information security and

compliance experience and in the past, he is associated with GE Healthcare, Philips Heathcare and many others. He is research scholar at GITAM university and his research interest include IoT Security. He has more than 23 certificates in infosec domain and published 11 papers in International journals and got 1 pending patent on his name.

Prof. V. Naga Lakshmi is heading the Department of computer science in GITAM (Deemed to be university). She published more than 18 technical papers in international journals and 21 technical papers in national and international conferences. She received various awards and recognitions for her research work that she carried throughout the career.