iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36977

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Security Concerns in Internet of Things

James Wenceslaus Ritte[1], Prof. Aryamol V.K[2]
[1]*School of Computer Science and Applications, REVA University, Kattigenahalli, Bengaluru, India*
[2]*Professor, School of Computer Science and Applications, REVA University, Kattigenahalli, Bengaluru, India*

Abstract: Security Concerns is the among of the significant challenges of Internet of thing (IoT). Lack of proper Device updates, lack of User awareness, Software compatibility issues, service disruption, inability to monitor their current status and software are Among the challenges that IoT is facing. In this work we are going to explore significant areas of IoT applications and security measures and identify management of Machine to Machine(M2M), Platform selection criteria, Knowledge of How data is managed on various IoT applications which includes (i) IoT in healthcare (ii) Blood Banks. In this work provide valuable insights into issues related to streamline workflows, predict necessary maintenance, analyze usage patterns, auto- mate manufacturing, and much more.

Keywords: Internet of Things IoT; security concern; cloud computing; edge computing; privacy

I. INTRODUCTION

A. Internet of Things

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. A thing in the internet of things can be a person with a heart monitor implant, a farm animal, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network. The new world of technology has afforded users with the ability to have a look on the status of their home security from their smartphones, to start their car with a mobile phone application, and to remotely open and close their garage door from anywhere in the world. These technologies are becoming part of what is known as the Internet of Things (IoT). In its most basic sense, the IoT refers to the connection of everyday objects (eg TVs, appliances, and exercise equipment) to the Internet. It enables the real time monitoring and vast collection of data about property, people, plants, and animals. Actually, smart homes and offices have become part of the IoT. Specifically, these smart homes and offices enable light switches, doors, windows, blinds, and temperature to be controlled remotely. On the other hand we have wearable devices like smart watches, (eg Fitbit versa) have been developed that can monitor individuals' activities and vital signs like heart beats.

II. MACHINE TO MACHINE (M2M)

M2M technologies represent closed, point-to-point communications between machines or between machine and management systems, without the need for human intervention. M2M devices, enabling bidirectional remote monitoring and transfer of data, consist of a sensor or a radio frequency identification (RFID) tag and a communication module.

M2M devices, as the industrial precursors to the IoT, can include items ranging from in-house/in-office machinery, such as printers or scanners, to manufacturing equipment, including heavy machinery.

But do not assume that the IoT will replace M2M. Predictions show that cumulative M2M connections will grow from 995 million in 2014 to a projected 2.7 billion connections by 2018. M2M uses include telemetry, traffic control, security, tracking and tracing, machinery maintenance and control, metering, and manufacturing and facility management, as well as a multitude of other applications. M2M/IoT will represent the next phase of the internet revolution, connecting about ten times more devices on the internet in a couple of years. So, it is best to be aware and start embracing it from its infancy and gain the first mover advantage.

III. EMERGENCE AND GROWTH OF IOT

The IoT establishes an end-to-end ecosystem, including technologies, processes, and concepts employed across all connectivity use cases. In principle, modern information and communication technologies play a vital role in IoT. As IoT is nothing but an exhaustive web of recognizable physical things, this will involve connecting not only humans but objects as well. These objects come with small processors and sensors like temperature controllers and audio or video output devices that are used to supervise the

surrounding objects. This helps to make the connected objects more responsive to the changes in the surroundings and thus to analyze the appropriate information or service to be provided, which makes our objects "smart".

The foundation of IoT is automatic identification through RFID. Sensors and actuators help by enhancing the applicability by encapsulating the real-time effects of actions. This leads to a huge opportunity for new services and applications in many areas. For instance, consumer goods may have a large repository of data which will help in providing a faster and more specific personalized service later on. Not only will this result in new business models and product innovations but it will also create a new line of products and services for more narrowed-down and specific customer needs, thus having a huge influence on individuals, markets, society, and enterprises.

The term *Internet of Things* was coined by Kevin Ashton while presenting RFID technology connected to the internet to easily identify products at Proctor and Gamble. The notion evolved and came to be more widely used in real life during the 2000s, especially after 2008, when the IPSO Alliance was formed to encourage the use of networked objects/things.

IV. CLOUD SYSTEM SELECTION

Often, the large number of devices that are typically deployed for an IoT application necessitates the use of a commercial cloud service that provides the performance and high-availability capability required by the application.

This requires customers to carefully ascertain whether the cloud provider has the right tools, cost models, and support for their needs. The right questions are not always clear since some aspect of their service or cost model may be appropriate until a certain size threshold is reached. This "scaling challenge" is often one of the most difficult areas of assessing what is possible.

V. IOT APPLICATIONS

A. Healthcare

It has been estimated that around 40% of the global economic impact of the IoT revolution will occur mainly in healthcare, as this sector is the one which requires the most surveillance and sensors. IoT-driven companies can gain a huge competitive edge in that sector—specifically in areas such as user experience, operational costs and efficiencies, and global expansion. With enormous potential to help patients as well as doctors, IoT-enabled devices are certainly the next big thing in healthcare and are here to stay for a very long time. Along with making patients feel safe and protected, these devices will also lead to greater patient satisfaction since they make interactions with doctors easier and convenient. The devices also help to shorten hospital stay length by providing real-time recovery assistance.

VI. IOT FOR PATIENTS

Estimates show that more than 200 million people in the European Union and the United States suffer from one or several diseases that may benefit from some type of home monitoring.

New IoT technologies are revolutionizing the way healthcare services are pro- vided, enabling patients to stay at home and receive the same service that would be provided at a hospital. Healthcare companies are extending their in-home services, delivering an easier life to those living independently, specifically tailored to serve senior citizens and disabled people worldwide. With that in mind, more and more state and federal healthcare agencies are promoting at-home care solutions as an essential way to enhance efficiencies and reduce costs.

Let us look at such a company named Simply Home, which designs and installs wireless/Wi-Fi technology products and similar healthcare-focused services. The company deploys a cost-effective IoT cellular solution that provides connectivity for its services, regardless of the patient's location. Its systems proactively alert patients and caregivers to alterations in day-to-day behavior by communicating with multiple sensors to observe a patient's everyday activities.

Text, email, or phone notifications can be triggered by a single activity, or many such activities, or by inactivity. Elements such as motion sensors, door/window contacts, and bed pressure pads alert caretakers to falls, wandering, or changes in sleep patterns.

The IoT-enabled Simply Home system helps residents stay carefree with environ- mental controls that switch on beds, lights, TVs, doors, and more via tablet or voice activation.

IoT is nothing short of a major milestone in elderly healthcare, mainly because of its feature of keeping a real-time track of the patient's health. It is a boon for elderly people living on their own or even with their families, as even a slightest change in the routine activities of the patient alerts both their loved ones and doctors.

VII. SMART METERING

Smart metering is among the primary steps to developing a detailed city-wide smart grid system that addresses challenges surrounding not only energy consumption but also water usage. This is possible through the help of real-time data tracking of electricity and gas usage, which is how smart meters enable utility providers to master energy distribution and at the same time also making sure consumers take smarter decisions regarding their energy consumption. Through the help of IoT solutions specially made for smart metering, customer service can also be improved substantially with the help of the insights provided by these IoT solutions, thus creating a win-win situation from every point of view.

Whereas traditional meters can only track total consumption, smart meters not only track total consumption but also provide information about the when and how of the consumption. This is exactly why power companies are now using smart meters to monitor consumer usage and price the energy according to the usage by dividing the consumption into different quotas.

VIII. RENEWABLE SOLAR ENERGY

According to the World Energy Outlook, around 1.2 billion people, roughly 16% of the global population, do not have access to electricity; about 95% of those people live in sub-Saharan Africa and developing Asia, and 80% live in rural areas. Hence, the need of the hour is to provide affordable, clean, and high-quality energy. For instance, BBOXX, a UK-based solar energy provider using IoT technologies, has developed solutions to provide energy to the less privileged in developing countries. By working with a carrier-agnostic and technology-agnostic partner, BBOXX installed a global subscriber identity module (SIM) at the point of manufacture, leading to both reduced supply costs and faster implementation.

Following suit is an Israeli company called SolarEdge with headquarters in the United States, which provides solar solutions for homes and businesses. Company products include power optimizers, solar inverters (DC to AC inversion), and cloud- based monitoring solutions. With a presence in 13 countries, all with somewhat different connectivity options and providers, secure and reliable connectivity was integral to the company's success. SolarEdge chose a carrier-agnostic and technology-agnostic IoT partner for deploying cellular connectivity, as well as for corresponding management solutions. Dealing with a seasoned, professional connectivity solution provider, SolarEdge was able to secure instant global connectivity and management oversight, advanced revenue-grade metering, and robust, real-time troubleshooting. Visibility into devices improved, operational efficiency rose, customer service radically upgraded, and inventory and loss management became transparent and easy to administer.

IX. CONCLUSION

The IoT connects and shares information about inanimate and living objects. Everything from medical devices and household appliances are being connected and be- coming part of the IoT. New and changing manifestations of vulnerability are present with the use of IoT and its pervasiveness in society.

The protection of IoT devices is a multifaceted and complex process. The existing risk of an inadequate legal framework requires urgent action in legal analysis and may require new approaches in legislation. To effectively deal with existing IoT vulnerabilities, it is recommended that a thorough analysis of the existing applicable legal framework is undertaken and that new elements are developed to address the risks related to IoT deployment, wherever needed.

X. ACKNOWLEGEMENT

I take this opportunity to express my heartfelt sincere thanks to Dr. S. Senthil, Professor & Director, School of Computer Science and Application , Reva University, my sincere thanks to Prof Aryamol V. K for her guidance and encouragement in carrying out this wonderful work, And also I am extremely grateful to my Father Wenceslaus O Ritte and my Brother Dr. Dismas W Ritte together with my Auntie Dorothy Mboya over encouraging and motivating guidance.

REFERENCES

[1] He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.

[2] Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.

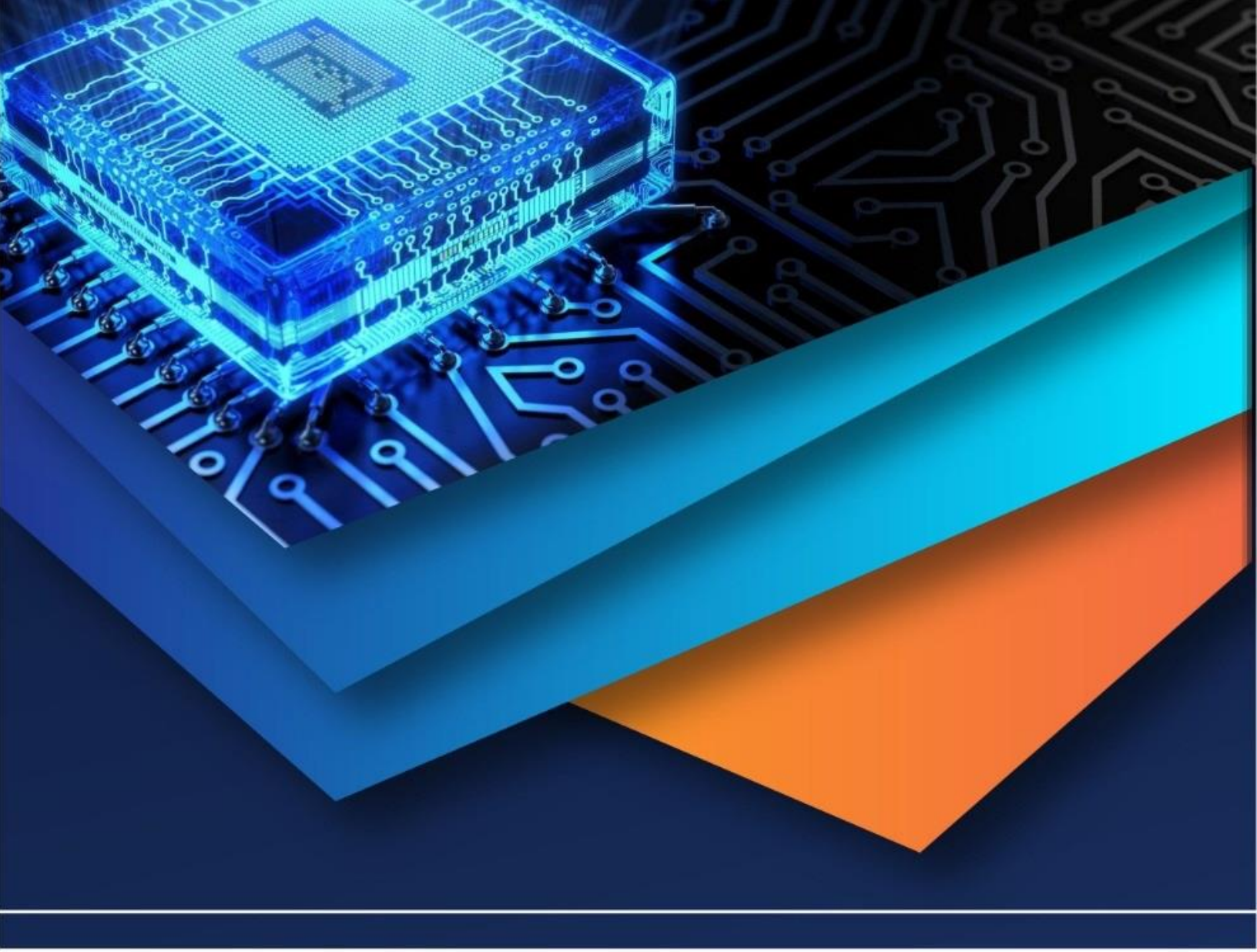
[3] Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. 2020, 11. [CrossRef]

[4] Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686 (accessed on 4 April 2020).

[5] Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342. [CrossRef]

[6] Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 2018, 74, 340–354. [CrossRef]

[7] Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eyers, D.M. Twenty security considerations for cloud- supported Internet of Things. IEEE Internet Things J. 2016, 3, 269–284. [CrossRef]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY