e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

INTERNET OF THINGS PRIVACY

Anjali Singh[*1]

[*1]Department Of Information Technology B.K. Birla College Of Arts, Commerce And Science Kalyan, Mumbai, India.

https://www.doi.org/10.56726/IRJMETS29639

ABSTRACT

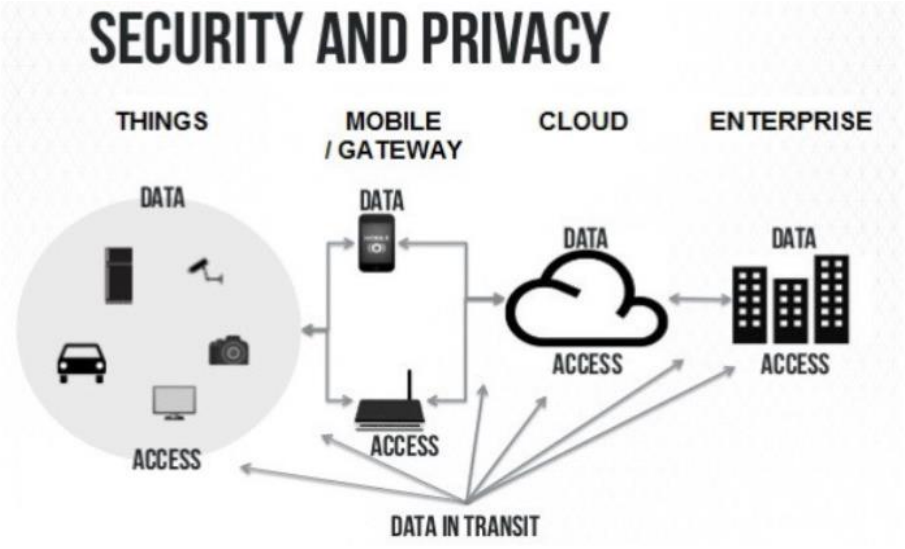
The Internet of Things is the intelligent connectivity of physical devices driving enormous gains in efficiency, industry growth, and quality of life. More things are being connected to address a growing range of business needs. In fact, till 2020, more than 50 billion things are connected to the Internets-even times our human population. Examples are wearable health and performance monitors, connected vehicles, smart grids, connected oil rigs, and connected manufacturing. This Internet of Things (IoT) will revolutionize the way we work, live, play, and learn. Inadequate security will be a critical barrier to large-scale deployment of IoT systems and broad customer adoption of IoT applications. Simply extending existing IT security architectures to the IoT will not be sufficient. The IoT world requires new security approaches, creating fertile ground for innovative and disruptive thinking and solutions. This survey summarizes the security threats and privacy concerns of IoT.

I. INTRODUCTION

The Internet of things Is the network of physical objects or things embedding electronic software and network connectivity, which enable these objects to connect and exchange data. The IoT allows the object to be sensed and controlled remotely across existing network infrastructure creating opportunities for more direct integration between the physical world and computer-based systems. When IoT is augmented with sensors and actuators the technology becomes an instance of the more general class of cyber-physical systems which also encompasses technologies such as smart grids, smart homes, intelligent transportation, and smart cities. Based on a large number of low-cost sensors and wireless communication, sensor network technology puts forward new demands on Internet technology. It will bring huge changes to the future of society, and change our way of life and business models.

Apart from the benefits of IoT, there are several security and privacy concerns at different layers viz; Front end, Back end, and Network. In this paper, the survey is on several security and privacy concerns related to the Internet of Things (IoT) by defining some open challenges. Then, discussion on some applications of IoT in the real world.

II. INTERNET OF THINGS (IOT) — SECURITY, PRIVACY, APPLICATIONS & TRENDS



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

If we want to understand the Internet of Things (IoT), let's have a look at the term "thing." Any physical device can be a "thing" (in terms of IoT). For example, it could be smartphones, washing machines, televisions, wearable devices, lamps, headphones, vehicles, buildings and anything possible that can be thought of. Shortly, it'll be true that "anything that can be connected will be connected."

Once we know what a "thing" is, let's examine the "Internet" part.

The things are embedded with software, sensors and other electronic components that help them send and receive data. The interconnectivity of these devices to the Internet and each other make IoT a giant network of connected "things." People are part of the network too. There are three kinds of relationships in an IoT network: things-things, people-things and people-people.

Now imagine a situation where we learn how the "things" are connected. Say you are returning from your office and wish that your air conditioner could be switched on before you reach home. What will you do? I know you will call your flatmate, mom or anyone who is present in your home to switch it on.

Now, let's think about the situation in terms of IoT. You will have a control station in your home, like a tablet or smartphone, to which you will send a message to switch on the air conditioner, and the smart device will communicate with the air conditioner and switch it on for you. This is the change that will be brought about by IoT. The connection between everything is IoT, sometimes referred to as the Internet of Everything (IoE).

III. IOT SECURITY AND PRIVACY CONCERNS

Although IoT is rapidly growing, it still faces security and privacy issues.

3.1 Security Risks

IoT devices are connected to your desktop or laptop. Lack of security increases the risk of your information leaking while the data is collected and transmitted to the IoT device. IoT devices are connected to a consumer network. This network is also connected to other systems. So if the IoT device contains any security vulnerabilities, it can be harmful to the consumer's network. This vulnerability can attack other systems and damage them. Sometimes unauthorized people might exploit the security vulnerabilities to create risks to physical safety.

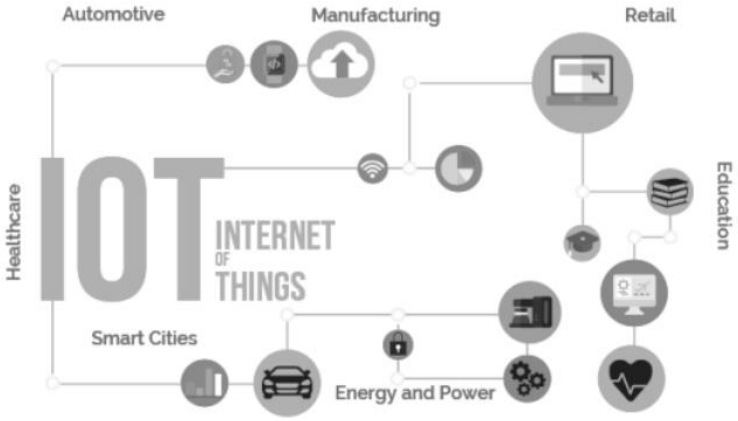
3.2 Privacy Risks

In IoT, devices are interconnected with various hardware and software, so there are obvious chances of sensitive information leaking through unauthorized manipulation.

All the devices are transmitting the user's personal information such as name, address, date of birth, health care information, credit card detail, and much more without encryption. Though there are security and privacy concerns with IoT, it adds value to our lives by allowing us to manage our daily routine tasks remotely and automatically, and more importantly, it is a game-changer for industries.

3.3 IoT applications across industries

Various companies now help businesses use IoT to solve long-standing, industry-specific challenges. They develop IoT solutions that connect things, collect data, and derive insights with open and scalable solutions that reduce costs, improve productivity and increase revenue. Let's see the industry categories, that are using IoT solutions in the figure below:



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

3.4 Trends in IoT

If we adopt IoT, it will improve the digitization of our society and economy by connecting objects, and people with each other via a connection or communication medium. If we consider device-to-device interaction, IoT helps people to manage their daily lives with more control with efficient monitoring. Let's see the trends in IoT app development areas.

Wearable gadgets: Wearable devices have been a hot topic across the tech world since the release of smartwatches and smart glasses. Today there are many wearable gadgets on the market, from fitness trackers to GPS shoes.

Connected Car: This is a quite new concept and is expected to come into the limelight slowly. Generally, app development for the automotive industry takes two to four years. Everyone from large-scale automobile companies to small-scale start-ups is working on connected car solutions. If BMW and Ford do not announce Internet-connected car solutions soon, the tech giants such as Google, Apple and Microsoft are set to develop and release the next generation of connected car solutions.

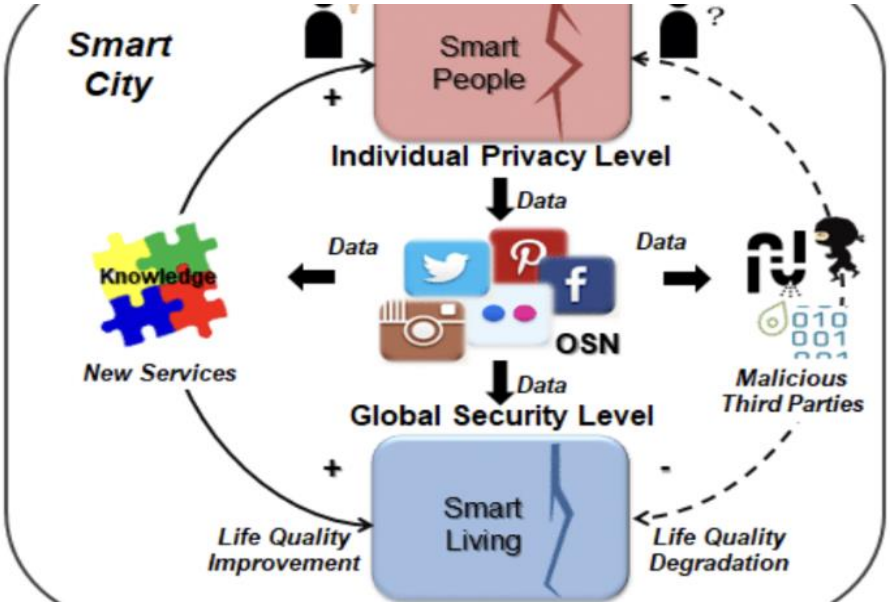
Smart Home: IoT provides us with a space where we find comfort and can manage our routine tasks easily in our daily busy life. There are various popular devices for the smart home; including smart thermostats, connected lights, smart fridges, smart television, smart door lock etc.

Smart City: Smart city helps people to avoid the issues of traffic management, social security, environment monitoring, waste management, water distribution etc. Improved IoT apps will help resolve various issues related to traffic, noise pollution, air pollution, etc., and make cities safer.

Along with these trends, the IoT market is booming with other emerging trends such as smart retail, industrial Internet, connected health, smart supply chain, smart farming, smart energy and so on. Even Artificial intelligence (AI) can enhance IoT with the help of the cloud platform.

IoT is also the chief enabler of Robotic Process Automation (RPA), systems that translate business processes into software-driven, rule-based decision trees. RPA provides cost savings and scalability advantages for businesses and shorter transaction times for customers.

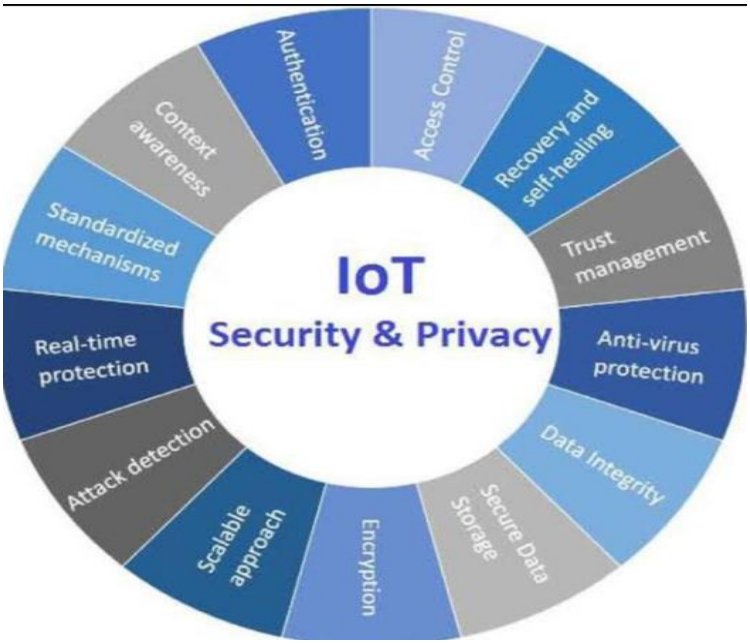
The rapid evolution of communication technologies, particularly in the area of IoT, involves also possible challenges far beyond the technological aspects, such as data protection and privacy are the upcoming challenges. Thus, the development of IoT offers the whole world an extended amount of opportunities.



IV. WHO IS RESPONSIBLE?

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the internet itself to potential harm. To scale up we need a collective approach to addressing security challenges on all fronts.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com



V. THERE ARE TWO WAYS TO VIEW IOT SECURITY

Outward Security

Focus on potential harm that compromise devices and system can inflict on the Internet and other users

Inward security

Focus on potential harms to the health safety and privacy of device user and their property streaming from compromised IoT devices and systems

Inward Security: What risks do secure IoT devices bring to Privacy and Security?

Using secure IoT devices increases the risk of personal data being exposed stolen and privacy compromised: A smart camera using a default username and password combination can be used to spy on you or be compromised to send a piece of junk information to the Internet variable smart device that sends health information over uninterrupted channels can expose personal data a smart home device like television that lacks sufficient updates can be a vulnerable to new attacks and can be used to share private data smart vehicle running in secure software can be accessed remotely and compromised to disable the certain function of the car.

Economic favor week IoT security

Strong security can be expensive to design and implement and it lengthens the time it takes to get a product to market. The commercial value of user data also means that there is an incentive to hold as much data for as long as possible. There is currently a shortage of credible ways for suppliers to signal their level of security to

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

consumers (e.g., certification and trust marks) The cost and impact of poor security tend to fall on the consumer and the other Internet users rather than on the producer of IoT systems.

How can IoT Security be improved?

Collaborative approach sharing of information by users, vendors manufacturers on security breaches and best practices. Strong policy controls for example: Requiring encryption in device IoT devices should use encryption to make it very difficult for a 3rd party to eavesdrop on communications framework on device features and capabilities. User education for example Train users on preferring stronger passwords on IoT device. Consumer demand for devices to have certain examples using two-factor authentication a password (something you know) and a token (something you have) Train users to identify an insecure device and avoid them.

How do we improve things?

- Research and Innovation
- Open Standards
- Certifications and Trust marks
- Policy and Regulation

VI. CONCLUSION

Recent challenges require new thinking avoid operational siloes networking and convergence are key to a sound security solution that is integrated throughout the build for the future Security must be pervasive inside and outside the network device- and data-agnostic proactive and intelligent Intelligence, not data convergence, plus analytics speed is essential for real-time judgments. We and the forthcoming generation must stand on the lookout for security and privacy because it should be our foremost concern to ensure that our data is secure.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

VII. REFERENCE

[1] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle - Privacy in the Internet of Things: Threats and Challenges.
[2] J. Sathish Kumar - A Survey on Internet of Things: Security and Privacy Issues.
[3] Rolf H. Weber - Internet of Things – New security and privacy challenges.
[4] Mikhail Kader, - IoT (Internet of Things) and Security- ITU Workshop on ICT Security Standardization.
[5] Elisa Bertino - Security and Privacy in the Internet of Things.
[6] Mark Mbock Ogonjia, George Okeyob, Joseph Muliaro Wafulac - A Survey on Privacy and Security of the Internet of Things.