# Internet to Things, Security and Privacy

**Shruti Vyas[1], Sagar Wankhede[2], Mayur Zodape[3], Divya Wagh[4], Prof. Sagar Tarekar[5]**
Students, Master of Computer Application[1,2,3,4]
Guide, Master of Computer Application[5]
Tulsiramji Gaikwad Patil College of Engineering, Mohgaon, Nagpur, Maharashtra, India

**Abstract:** *The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT*

**Keywords:** Security, Privacy

## I. INTRODUCTION

Security and Privacy, two words that we all can agree are vitally important and an integral part of any successful society. That makes it sound like we're going to dive deeply into philosophy, politics, and culture – but we're not deliberately going there. However, because these topics (which are two sides of the same coin) rely heavily upon what is and is not legal, what is and is not moral, and what is and is not culturally viable, the discussion will inevitably include aspects of each of these from time to time.

When we've talked about security and privacy before, we've heard opinions that we're being "paranoid", or "if you have nothing to hide, you have nothing to fear", and other commentary trying to stigmatize the overall concept of privacy as crazy, insane, or just plain silly. This isn't the forum for that kind of criticism. To help set the stage for this discussion, let's define some terms, so we're all using the same terminology.

## II. UNDERSTANDING THE CONCEPT OF SECURITY IN IOT

Now that you know about the importance of security and privacy for the long-term growth of IoT, it is reasonable to reflect on both of them individually. What are the factors associated with the concerns of security in IoT? The Internet of Things landscape is gradually becoming more diverse with legacy computing systems and modern computing devices. As a result, IoT easily becomes vulnerable to a wide range of security risks in different approaches.

First of all, it is important to note that many devices in the IoT landscape are tailored for large-scale deployment. The example of such devices refers to sensors. In addition, deploying IoT devices also involves a set of similar or almost identical appliances with resembling traits. The resemblance is responsible for magnifying the security vulnerabilities. While security issues have been prominently noted in the information and technology sector, IoT implementation has come up with some new challenges.

The answer to 'Why security is important in IoT?' is evident in the nature of interconnectivity between the IoT devices. If a poorly secured device connects with the IoT landscape, then it could affect the security and resilience of IoT. With a large number of homogenous devices deployed in IoT, the IoT users and developers must ensure that they are not exposing other users to potential harm.

One of the most prominent factors to draw your attention towards security in IoT would refer to authentication. The authentication mechanisms used in existing IoT ecosystems are restricted only to offering safeguards against limited

DOI: 10.48175/IJARSCT-9147

ISSN
2581-9429
IJARSCT

threats such as replay attacks or Denial of Service (DoS) attacks. It is also important to consider the role of information security as one of the highly vulnerable domains of IoT authentication. Why?

The abundance of risky applications which enable a natural multiplicity of data collection could present formidable information security risks. In addition, the importance of security becomes clearly evident with the prevalence of man-in-the-middle attacks. Third-party agents could intercept communication channels for impersonating identities of vulnerable nodes associated with network exchange.

## III. UNDERSTANDING THE CONCEPT OF PRIVACY IN IOT

The next notable aspect in discussions on privacy and security in IoT refers to the way consumers view privacy. People are likely to perceive the usefulness of IoT in accordance with its effectiveness in safeguarding their privacy goals. The common assumptions regarding privacy issues in IoT and the potential security issues could become formidable setbacks in IoT adoption.

The aspects of user privacy and the rights of privacy are basic requirements for developing the trust and confidence of users in IoT, connected devices, and associated services. At the same time, the developments in IoT are focusing largely on addressing privacy issues in a completely new way.

One of the most important concerns in understanding the issues of privacy in IoT would draw attention towards reasons for privacy concerns. The IoT ecosystem has intelligent artifacts present almost everywhere with flexibility for sampling process and information distribution from any location.

In addition, the ubiquitous connectivity in IoT through the internet also plays a crucial role in amplifying privacy concerns. Without a unique mechanism for privacy protection, the ubiquitous connectivity of IoT could enable flexible access to personal information from any corner of the world.

## IV. CONFIDENTIALITY, INTEGRITY, AVAILABILITY

The following is a breakdown of the three key concepts that form the CIA triad:

- **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

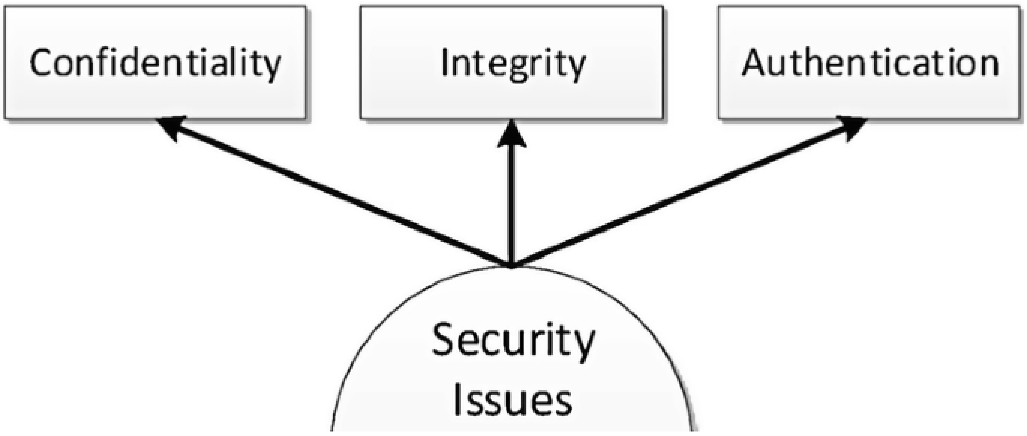

Fig: Security Issues

DOI: 10.48175/IJARSCT-9147
ISSN 2581-9429 IJARSCT

Privacy concerns with social networking services is a subset of data privacy, involving the right of mandating personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information pertaining to oneself via the Internet.

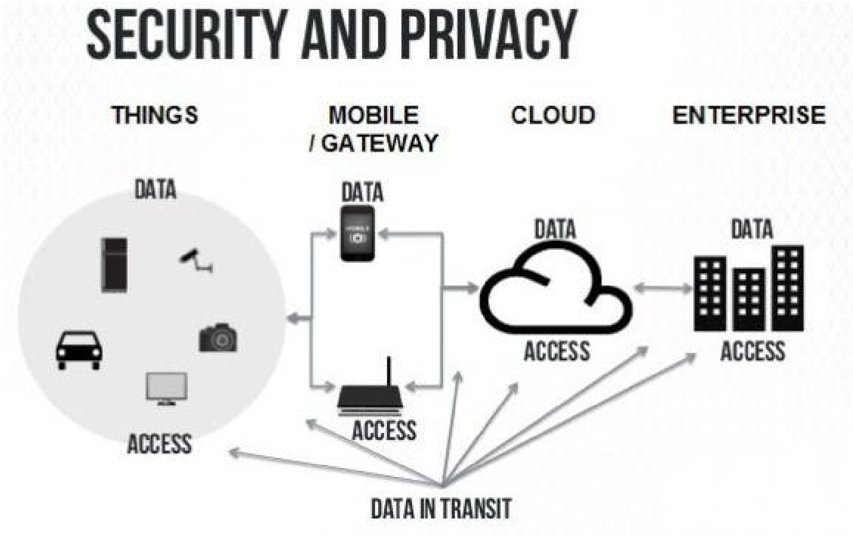

Fig : Security and Privacy Measures

## V. IOT SECURITY AND PRIVACY CONCERNS

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

**Security Risks**

- IoT devices are connected to your desktop or laptop. Lack of security increases the risk of your personal information leaking while the data is collected and transmitted to the IoT device.
- IoT devices are connected with a consumer network. This network is also connected with 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.

**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 card information, credit card detail and much more without encryption.

Though there are security and privacy concerns with IoT, it adds values 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.

## VI. 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:

DOI: 10.48175/IJARSCT-9147
ISSN 2581-9429 IJARSCT

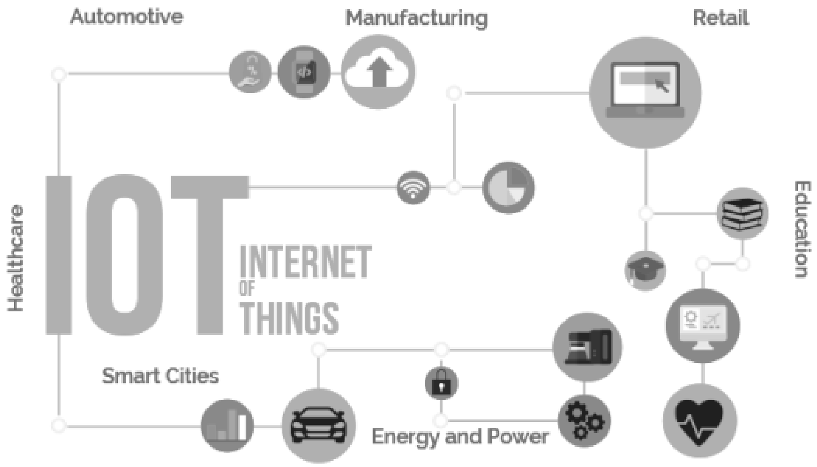

Fig : IOT Application

## VII. TRENDS IN IOT

If we adopt IoT, it will improve digitization of our society and economy by connecting objects, people with each other via a connected or communication medium. If we consider about 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 glass. Today there are many wearable gadgets on the market, from fitness trackers to GPS shoes.
- **Connected Car:** This is a quite new concept and 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 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; include smart thermostat, connected lights, smart fridge, 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.
- **Smart Grid:** It is a vital niche of IoT. It provides information about consumers and electricity providers in an automated way. It always helps improve the efficiency, economics and electricity steadiness.

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) has the capacity to 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.

## VIII. DISCUSSION

Security and privacy issues has a significant impact on the adaptation of IoT. The growing research in this area should consider the security and privacy requirements at each layer and at each development point and address them. As the

ISSN 2581-9429 IJARSCT

number of connected heterogeneous nodes increase rapidly and most of the data in the IoT is sensitive and/or personal data, the challenges facing the complexity of the implementation of security solutions are rising. IoT is easy to attack at each layer which makes tackling the security issues a critical area of research. IoT security main requirements include: confidentiality, authorization, authenticity, integrity, and availability. Security challenges in IoT such as service quality, confidentiality and reliability, confidentiality, managing and securing big data, software and hardware vulnerability and creating relevant standards are still open issues and not fully addressed [9]. Authentication and identification are fundamental for IoT data privacy, which is also a main security issue in IoT.

However, it faces many neglect while it must be preserved at each part of IoT. Protecting IoT require appropriate security frameworks that covers all IoT layer-security issues. Further research is needed to develop and design proper security solutions for IoT that considers the limitation of its devices. In addition, there is a need for developing a holistic security and privacy frameworks that tackle the identified issues at each layer and consider influencing factors.

## IX. CONCLUSION

Along with an exponential growth in connected devices, each thing in IoT communicates packets of data that require reliable connectivity, storage, and security. With IoT, an organization is challenged with managing, monitoring, and securing immense volumes of data and connections from dispersed devices.

## REFERENCES

**[1].** By RH Weber • 2010
**[2].** https://www.sciencedirect.com/science/article/abs/pii/S0267364909001939
**[3].** https://medium.com/@arindey/internet-of-things-iot-security-privacy-applications-trends-3708953c6200#:~:text=Security%20Risks
**[4].** https://101blockchains.com/security-and-privacy-in-iot

DOI: 10.48175/IJARSCT-9147
ISSN 2581-9429 IJARSCT