Security in the Internet of Things (IOT)

Venkata Sathish T[1], Sreedevi M[2]

[1]Dept of Computer Science, S V University, Tirupati
[2]Assistant Professor, Dept of Computer Science, S V University, Tirupati

Abstract**—** *The economy's backbone is technology. In today's world, there has been a shift in the paradigmatic approach to information technology, with Innovation, Internet of Things, Social, Mobility, Analytics, and Cloud services emerging as the fastest expanding verticals, shaping the future of the country's IT and Electronics sector growth. Policies must be considered and notified, preferably simultaneously or in close succession, in order to provide a comprehensive picture of what the country wants to achieve and how it intends to do it. Infrastructure, Human Capital, Incentives, and Good Governance are the four pillars on which these policies are built.*

Keywords: IoT, Devices, Policies.

I. INTRODUCTION

The Internet of Things (IoT) is a web-based information architecture that allows for the secure exchange of goods and services. In other terms, the Internet of Things (IoT) connects physical devices and their knowledge representations to enable the exchange of "things" across a secure network architecture. In global supply chain networks, the main benefit of IoT is comprehensive transparency and transaction efficiency. IoT, according to Haller, Karnouskos, and Schroth, is a system that connects physical things to information and communication networks and encourages smart devices to participate in business activities. For the past year or so, secure IoT services have been progressively emerging.

Grid computing and cloud computing are similar to distributed computing. IoT can also be thought of as a sort of ubiquitous computing, in which the entire information space becomes a smart environment that observes, detects, adapts, and collates numerous items.

Using the principles of IoT, any physical thing might be made smart enough to interact and communicate with other objects.

It is no longer necessary to create smart objects, but it is feasible to make any object smart.

Many examples can be given to illustrate the notion of IoT and its applications. Any other thing, such as a car, a refrigerator, an umbrella, or simply a chair and a pen, can interact with a cell phone. Object-to-object interaction can be done in either half-duplex or full-duplex mode. Because humans are not things, the Internet of Things is not directly linked to them. Humans, on the other hand, may monitor, control, and benefit from IoT. RFID, GPS, barcodes, and other technologies that are now accessible could be useful in the development of IoT.

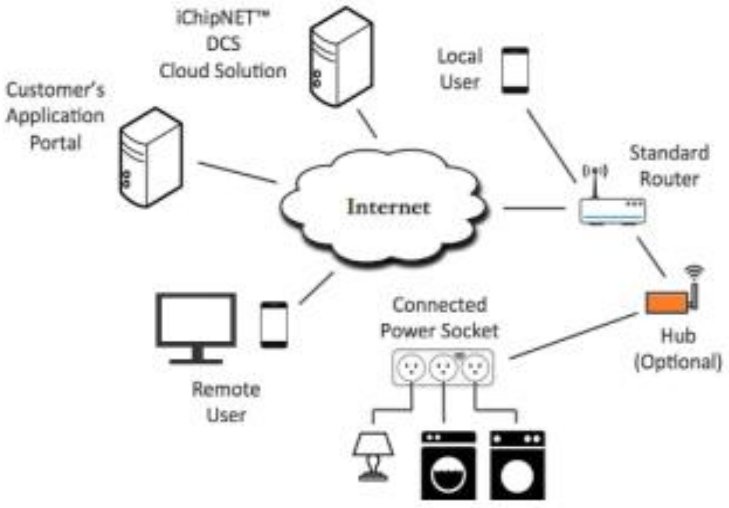


FIGURE 1: Block Diagram of IOT

The government of India's smart city plan envisions the constructive use of IoT in practically every aspect of life. Pentagram Research Centre Private Limited, a Hyderabad-based firm, and Avatar Med Vision US LLC, NC, a US-based firm, have proposed three initiatives: The Digital Food Initiative, the Digital Health Initiative, and the Digital Security Initiative, all of which would focus on advanced IoT tenets (Ref: www.pentagramresearch.com). These three programmes are focused on specific parts of smart cities, or to be more specific, smart countries. The following is a list of some of them.

1. IoT enabled corporate farming
2. IoT enabled transportation of things and people
3. IoT enabled Farm-To-Home (FTH) distribution system
4. IoT enabled power distribution system 5. IoT enabled health care
5. IoT enabled security measures
6. IoT enabled governance

II. IMPLEMENTATION OF IOT

Internet of Things (IoT) is implemented in three Stages

- Implanting appropriate sensors on objects and allocating addresses to them.
- Sensor data collecting and aggregation software.
- Expert systems are used to transmit data and make decisions.

Many countries, including Korea, Denmark, Switzerland, and the United States, have already taken steps to develop IoT-enabled infrastructure and services. The following are the steps that must be followed in order to adopt IoT.

1. In this framework, investment in fundamental research and development is critical.
2. It is critical to manufacture sensors for diverse data collection purposes.
3. Multi-sensor fusion approaches must be further investigated.
4. The use of big data analytics approaches to format raw data will be investigated.
5. Decision-making techniques based on machine learning must be developed.
6. Human resource training in this area should be taken seriously.
7. Policymaking in the public and private sectors is critical for network integration.
8. For the initiative's own survival, it must be given a commercial perspective.

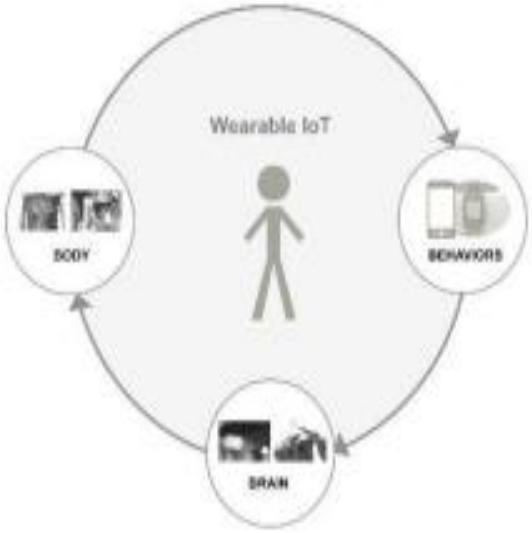
III. APPLICATIONS OF IOT AND CHALLENGES

Some of the applications of IoT are briefly described in the following:

3.1 Wearable Technology & Personalized Healthcare

Wearable technology that collects data from physical activity monitoring and responds in real time is the future of personalised healthcare. Wearable gadgets can measure temperature, heart rate, blood pressure, and movement abnormalities, as well as dispense medication.

Within five years, biometric information about humans will be available in the network, allowing devices and diverse physical things to warn and advise humans on corrective actions based on situation-relatedbiometricdata.



3.2 The Connected Home

Home automation is a ten-year-old paradigm that will play a key part in connecting all homes in a city and all cities throughout the country. Users will soon be able to operate all household electronics with just their phone, if current trends continue. People are now utilising technology for longer amounts of time than they sleep, according to studies, as the capacity to multi-task tasks with smart phones and tablets improves. Users can save energy in their homes even when they are not present thanks to this level of remote control and access in the palm of their hand. The simplicity of doing so with a simple interface and connecting several devices.

Individuals will benefit from the devices and programmes not only in terms of saving money, but they may also have an environmental impact by lowering energy use and, ultimately, climate change. A smart lock does not need to be connected to the internet, and users can still use their traditional keys. The door would be opened by a signal from a smartphone app. Homeowners may use the app to transmit digital keys to friends and relatives, as well as delete them as needed.

3.3 Smart Cities

A smart city is a vision for urban development that aims to ensure the integration of numerous information and communication technology (ICT) solutions to manage a city's assets.

Local department information systems, schools, libraries, transit systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services are among the city's assets. The purpose of constructing a smart city is to improve people's quality of life.

By utilising technology to increase service efficiency and satisfy the requirements of local's ICT allows city officials to connect directly with the public and city infrastructure, as well as monitor what is going on in the city, how it is evolving, and how to improve the quality of life. Data is collected from citizens and gadgets using sensors connected with real-time monitoring systems, then processed and evaluated. The data and insights acquired are crucial in combating inefficiencies.

Here, then, are the top 10 smart cities on the Planet:

1. Vienna.
2. Toronto.
3. Paris
4. New York
5. London
6. Tokyo
7. Berlin
8. Copenhagen
9. Hong Kong
10. Barcelona

The Indian government's goal to build 100 smart cities across the country, for which Rs. 7,060 crores have been set aside in the current budget, could result in a vast and rapid expansion of IoT in India. In addition, the government's Digital India Program, which aims to "convert India into a digitally empowered society and knowledge economy," would give the necessary momentum for the country's IoT business to grow. The many initiatives outlined under the Smart City idea and the Digital India Program to establish Digital Infrastructure throughout the country would aid the IoT business. The Internet of Things (IoT) will be important in making these cities smarter.

Cities now house more than half of the world's population, and the need to make future cities more intelligent and connected has never been stronger.

A crucial question is how future cities might be better structured to benefit healthcare, education, transportation, and energy demands.

When natural and environmental conditions are taken into account when constructing IoT enabled smart cities, future smart cities will be "flexible." A decision made for the dynamics of a smart city in one season does not have to be repeated in another.

Furthermore, a white area for researchers and city planners is an expert system-based autonomous control over the dynamics of future smart cities.

IV. SECURITY AND PRIVACY CHALLENGES

In most countries, there are no regulations that particularly address IoT devices, thus when a firm wants to gather data from users, it must abide by basic privacy laws, many of which were enacted before the phrase "IoT" was coined.

Privacy regulations differ from country to country, which can be difficult to navigate. For example, corporations situated in the United States used to be allowed to readily gather data from consumers in the European Union (EU), where data privacy laws are stronger, if they were certified under the Safe Harbor programme. However, the EU ruled Safe Harbor ineffective late last year. "Companies have had to hurry to have some backup mechanism in place to make the data transfers legal," said Kate Lucente, a US attorney who specialises in data privacy problems.

As the transition from closed networks to open enterprise networks accelerates and the use of smart devices grows, several concerns about data security have arisen. How will we successfully monitor and protect personal information and public safety as IoT technologies become more widely used and our reliance on interconnected devices grows?

The primary goal of the Internet of Things is to create an autonomous world order with minimal human intervention.

Devices and objects may be intelligent, perhaps even smarter than humans, but they are not bound by emotions. Human beings, on the other hand, operate primarily through emotions, making any system in which humans play a role vulnerable to corruption and abuse. This translates to any autonomous system that includes humans as a component posing a threat to the system's integrity. As a result, the most significant risk in an IoT-based system is a security compromise, which might result in chaos and disaster.

V. EMERGING TRENDS & OPPORTUNITIES IN THE IOT

Despite the fact that work on sensor development and big data analytics is underway, it is far more critical that basic research in fields such as environmental engineering, natural disaster prediction in disaster-prone areas, and post-disaster damage control be undertaken.

Manufacturing will be more efficient as a result of improved supply chain management; healthcare will be impacted by increased patient surveillance; agriculture will be improved by monitoring crops and controlling growing conditions; our environmental data will be captured and controlled to reduce air pollution; and water leakages will be detected using sensor devices, to name a few.

The existing Internet of Things security is not as good as it should be. This thesis demonstrates some obvious problems in existing products, which are frequently caused by developer carelessness, as the limits present in IoT necessitate a more complete thought process than is typical in desktop computing. Because of the restricted amount of power, bandwidth, and processing capacity available, everything must be pared down to the basic essentials while still keeping good security properties.

VI. SUMMARY

In many initiatives, security is overlooked. Using examples from past research and completing unique analysis on current products, it is demonstrated that many developers either ignore or construct their own encryption methods with obvious faults (BMW, Home Easy, Sonos) (Eye-Fi, OSGP smart grid).

This paper attempts to have developers think about the constraints that exist, and propose answers to the challenges that may arise when developing a device for the Internet of Things, in order to ensure that the future of IoT is secure.

Consumers care about the security of the Internet of Things.

The majority of consumers (62 percent) "feel fully violated and incredibly upset to the point where I would take action" as a result of not focusing on the security of IoT devices, according to prior study.

Nearly half of all consumers (48 percent) would hold the maker liable if a weakness was discovered in the system, demonstrating the clear financial dangers involved in not properly protecting a gadget.

Some of the difficulties discussed are familiar in the field of information security, but they bring novel challenges due to the specific limits. Confidentiality, integrity, and authorisation are all required for an IT system to be secure. Choosing an encryption, authentication, and signature scheme is not as simple as calling a different method, as it is normally handled by libraries like OpenSSL and employing TLS into desktop PCs. Because of the device's limited power, bandwidth, and processing capabilities, it will necessitate a careful thought process to determine how to secure it both efficiently and effectively.

The other challenges are more Internet of Things-specific. An advanced user interface is frequently available in conventional desktop computing, and physical device loss during use is uncommon. IoT devices, on the other hand, typically have very restricted user interfaces and are frequently put in exposed areas and used in high-stress scenarios.

Throughout the process, security should be a priority. Key security considerations should have been made long before the initial prototype PCB design is shipped to the manufacturing. These include things like how keys should be distributed to each device, if hardware acceleration should be used, how updates should be handled, whether a public key infrastructure is a viable solution for the device, and what cryptographic methods should be employed, among other things.

VII. FUTURE WORK

In terms of optimum protocols and security, the Internet of Things is a relatively new concept, therefore there is a lot of work ahead of it. The most important challenge is making security in IoT easier for developers who don't have extensive expertise of IT security. For the future of IoT, designing and implementing security in protocols that are easy to use by developers is a necessary. In the Internet of Things, speed and cryptographic strength are very crucial.

Because devices in the Internet of Things are restricted, efficient implementations of cryptographic algorithms are critical for maintaining acceptable cryptographic strength.

The Internet of Things (IoT) is a rapidly evolving field that will continue to do so in the future. While the recommendations in this thesis are based on predictions about the future of IoT and cover a wide range of solutions, they will need to be revisited if the market changes significantly. However, because many cryptographic features will always exist and be relevant, the majority of the suggestions will remain unchanged in the near future.

VIII. CONCLUSION

The Internet of Things (IoT) is the future of globalisation, and Western countries have already begun to implement various strategies and projects in this area. India, as is customary, lags behind them, and it is past time for the country to begin thinking in this way.

This is a show of unity and integrity, and the federal and state governments should recognise it by providing plans and facilities to various government and private companies. The common guy should likewise be educated in this manner.

REFERENCES

[1] Sophie Curtis, Director of Marketing at RE•WORK

[2] http://www.windriver.com/whitepapers/security-inthe-internet-of things/wr_security-in-the-internet-ofthings.pdf.

[3] Draft Policy on Internet of Things, Department of Electronics & Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India

[4] http://siliconangle.com/blog/2014/03/21/mostinfluential-countries-for-the-internet-of-things/ by Mellisa Tolentino | Mar 21, 2014

[5] https://arc.applause.com/2015/12/02/internet-ofthings-growth-developing-countries/

[6] ZDNet Korea (zdnet.co.kr)

[7] www.aponline.gov.in/apportal/Downloads/2016ITC_ M S3.pdf

[8] Rolf H. Weber, Romana Weber - Internet of Things.pdf by Springer Publications Security in Internet of Things Systems by Christian Dancke Tuen, Norwegian University of Science and Technology.

[9] The Internet of Things: An Overview by Karen Rose, Scott Eldridge, Lyman Chapin.