Emerging Trends in IoT with Data Mining

G. Jeya Sutha Perciya
Assistant Professor
Department of Information Technology
Pope's College, Tamil Nadu, India

Abstract— Internet of Things is a world beyond of interconnected things which are capableness of sensing, actuating and communicating among themselves and with the situation (i.e., smart things or smart objects) while providing the ability to share information and act in parts autonomously to real/physical world events and by triggering processes and creating helpful action or without direct human intervention. It has been rising speedily due to recent progresses in communications and device technologies. Interfacing an each item together through internet features very hard, but within a construction of time IoT will radically alteration our lifetime. By attaching the information with things (devices) and using the Internet we can achieve the communication between devices to devices.

Key words: Attacks, Cryptography Algorithms. Internet of Things

I. INTRODUCTION

With technical advancements, our interaction with information systems is changing, both at work and during leisure time. Information, sensor, and network technology are fetching progressively small, more powerful, and more frequently used. People no longer only encounter information technology at common points in their lives, such as in offices or at desks, but as information and communication structures, which exist in increasing areas of everyday life. These structures are categorized by the fact that they not only contain standard devices, for example, system and mobile, but that data and communication process is also entrenched in objects and surroundings. According to another definition, The IOT has been defined in many ways. Generally Communication, it refers to a global, distributed network (or networks) of physical objects that are proficient of sensing or substitute on their location and able to communicate with everyone, other machines or systems. Such 'smart' objects come in a broad range of sizes and dimensions, including simple objects with embedded sensors, home Appliances, manufacturing wearable objects such as wristwatches, Ornaments or tops [1]

II. FUNCTIONALITY OF IOT SOLUTIONS

Internet of Things is sometimes assumed as being identical with smart systems [2]: elegant wearable, smart households, smart metropolitan city, smart environment and so on. This Subdivision confers the functionality evaluation of IoT solution available in different areas.

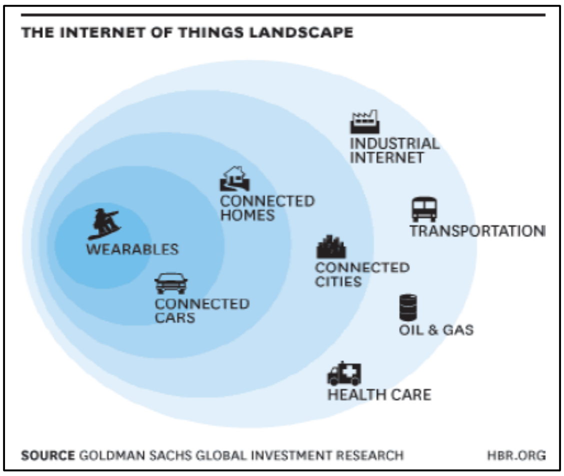


Fig. 1:

A. *Smart Wearable*

Smart wearable are networked campaigns that can gather data, track events, and customize capabilities to users' needs and wants. A IoT technologies related to Smart household are emerging.[5]. Solutions in this category make the experience of living at home more convenient and pleasant for the Wearable solutions are considered for a collection of functions as well as for where on a distinctive of part of body such as the head, eyes, wrist, waist, hands, fingers, legs or embedded into different element of costume. [3]. One standard is constructed on product forms, including head-mounted (such as glass and helmet), body-dressed (such as coat, underclothing, and jeans), hand-worn (such as wristwatch, bracelet, and handbags), and bottom - worn (such as shoes and socks). Another standard is based on product functions, including healthful living (such as sport wristband and smart bracelet), information accessing (such as smart glass and smart watch), and somatosensory mechanism (such as somatosensory controller). [4]

B. Smart Homes

Smart Homes Smart Home is the combination of technology and facilities concluded home networking occupants. Some smart home solutions also emphasis on support elderly Hand (Gloves), Finger(Rings), Wrist(Watch/Bands), Eyes(Spectacles), Feet (Socks), Base (Shoes), Head (Hat), Body(Material), Waist(Band), Chest(Band) people in their daily activities and on well-being care observing. Due to the large market potential, new and more smart home resolutions are making their way into the market. From the academic point of view, smart energy and resource management, human–system interaction, and activity management have been some of the major focus. [6]

C. Smart City

A 'smart city' is an town region that is highly progressive in terms of overall structure, maintainable real estate, communications and marketplace feasibility. It is a city where communication technology is the principal infrastructure and the basis for delivering essential services to populations. There are many technological proposals involved, including but not reduced to systematized sensor networks and data centers. Urban IoTs, in fact, are designed to support the Smart City vision, which aims at exploiting the most advanced communication technologies to support added-value services for the administration of the urban and for the citizens. The purpose of the IoT pattern to an urban context is of particular interest, as it returns to the strong push of numerous national governments to implement ICT solutions in the management of public dealings, thus realizing the Smart City concept.

D. Smart Environment

The Smart Environment in a city comprises of Smart Governance, Impertinent Mobility, Smart Efficiencies, Smart Buildings.[8].Services enabled by the IoT standard in smart city atmosphere might ranges from Observing well-being structure, Management of unused, Observing air quality, Observing noise, Traffic obstruction ,smart parking , smart lightning, water quality observing, natural failure monitoring ,smart agronomy and much more. For instance, Air quality egg[9] is a community led sensor system that helps the community to have better air quality. [10] There are various solutions available offering separate solutions in different areas.

E. Smart Enterprise

Enterprises IoT resolutions are premeditated to support infrastructure and more general purpose functionalities in industrial place. Modern enterprise approaches previously acknowledge rare boundaries to smart items, but with improved computational and communication abilities of these items, the power shifts towards the boundaries of the network. Intelligent mechanisms for data accumulation, filtering, synthesis and conversion can be organized to and implemented at the network edge, or within the network, as proper. Software is previously the key revolution driver in many trades and many new business models of the future will severely rely on the use of such items.

ome of the most promising ones are Manufacture, supply chain integrity, resources and production, health, transportation and logistics.

III. STRUCTURAL DESIGNS OF INTERNET OF THINGS

From the perspective of architecture, the IoT can be generally split into three layers, namely perception layer, network layer, and application layer. The perception layer renovates the information of things to the understandable digital signals via RFID, sensors, etc.

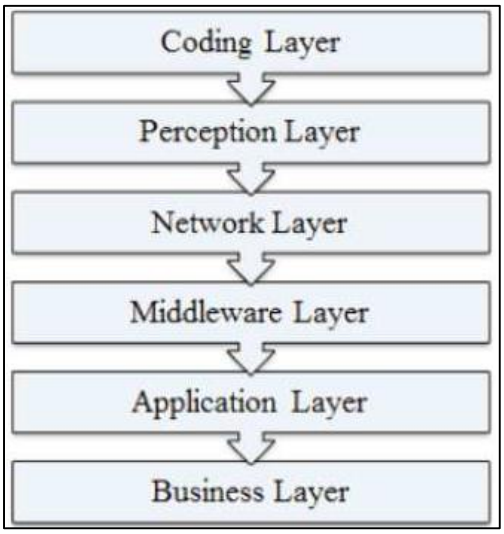


Fig. 2:

A. Coding Layer

Coding layer is the bottom of IoTs which gives fundamental recognition to the devices that are part of Internet of Things. In this layer, every devices are assigned with "unique ID" which creates it simple to distinguish the devices [11].

B. Perception Layer

Perception layer of IoT, which provides a objective meaning to every device. It contains of data sensors indifferent forms which could sense the humidity, temperature, location and rapidity of the device. This layer gathers the information of the device from the sensor linked with them and translates the information into digital signals which is then carried onto the Network Layer for advance action.

C. Network Layer

The purpose of Network Layer is accept the valuable information in the form of digital signals from the Perception Layer and transmission it to the processing systems in the Middleware Layer over the trans-mission mediums like Bluetooth, WiFi, 3G, GSM, etc. with protocols like IPv6, IPv, etc. [12].

D. Middleware Layer

Middleware layer processes the data expected from Network Layer . It contains the technologies like Global computing, Cloud computing which provides a open log on to the database to record all the essential information in it. Using some Smart Processing Equipment, the information is managed and completely automated action is occupied based on the treated results of the information.

E. Application Layer

Application layer identifies the applications of IoT for all types of production, constructed on the governed data.
Applications promote the progress development of IoT so this layer is very useful in the enormous scale development of Internet of Things network. The Internet of Things applications could be smart transportation, smart homes, smart planet etc.

F. Business Layer

Business Layer dominations the services of IoT and application and is responsible for all the study narrated to Internet of Things. It builds different business models for different business approaches.

IV. STRUCTURAL DESIGN OF IOT IN HEALTHCARE

IoT is a concept which is still at very early stages, where everybody translates the vision with their own perspectives. There are three main visions of IoT based on the things, digital and semantic viewpoints. All these three evaluations of IoT should combine with each other seamlessly as shown in the following Figure, for isolating the full benefits of IoT structure.

A. Things Integration
B. Data Integration
C. Semantic Integration

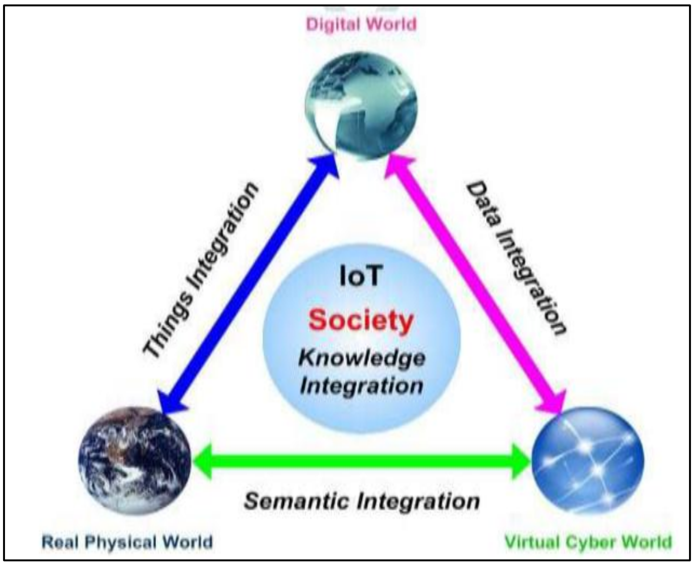


Fig. 3:

A. Things Integration

This integration provides the prospect that all the real physical objects can have the sensors supporting to get the actual time information from them. This can be accomplished by the sensors centered network of embedded electronic devices using RFID, NFC and other wireless technologies. This vision provides the base for integration of all "things" using distinctive sensor based networks to cooperate and co-exist together.

B. Data Integration

This integration provides the prospect that all the devices can be associated through internet and can be defined as smart objects. This can be accomplished by using unique IP for each connected object. This integration provides the base for the data integration of all the smart objects, which can be constantly monitored.

C. Semantic Integration

This integration provides the prospect that all the data collected from carious sensors need to be examined for expressive explanation. This can be accomplished with semantic techniques, which separates raw data from the significant data and their interpretation. This vision offers the base for the semantic integration over the use of semantic middleware.

V. NEED OF SECURITY IN IOT

Among these three layers, security is a difficulty to ensure signal is altered collected, transmitted, and translated by the applications. Both the ordinary nodes and sink nodes are exposed to a variety of security attacks, such as rejection of service attacks, or banned control and failure. These attacks could concession the sensitive information and result in malfunctions.[13]

A. Types of Attack on IOT

1) Physical Attacks
2) Side Channel attacks
3) Cryptanalysis attacks
4) Software Attacks
5) Network Attacks

1) Physical Attacks

These types of attacks interfere with the hardware components and are somewhat harder to perform because they requires an pricey material. Some examples are de-packaging of chip, layout renovation, micro-probing, particle beam techniques, etc.

2) Side Channel attacks

These attacks are constructed on a side channel information that can be recovered from the encryption device that is neither the plaintext to be encrypted nor the cipher text resulting from the encryption process. Encryption devices construct timing information that is easily quantifiable, radiation of various sorts, power spending statistics, and more.

3) Cryptanalysis Attacks

These attacks are determined on the cipher text and they try to breakdown the encryption, i.e. find the encryption key to obtain the plain text. Examples of cryptanalysis attacks include cipher text only attacks, known-plaintext attack, chosen plaintext attack, man-in-the-middle attack, etc.

4) Software Attacks

Software attacks are the main source of security susceptibilities in any system. Software attacks deed implementation vulnerary system through its own communication interface. This kind of attack includes developing cushion overflows and using Trojan horse programs, worms or viruses to deliberately inject malicious code into the system.

5) Network Attacks

Wireless communications systems are exposed to network security attacks due to the transmission nature of the transmission medium. Basically attacks are organized as active and passive attacks. Examples of passive attacks include monitor and eavesdropping, Traffic analysis etc.

VI. CRYPTOGRAPHIC ALGORITHM

There are several cryptographic algorithm offered based on key distribution conventional cryptography is stated to as Conventional cryptography is stated to as symmetric encryption or single key encryption. Similar key is used for encryption and decryption. This method of encryption key is equal to the decryption key. Figure represents the simplified model for conversional encryption technique. In general, there are two kinds of the symmetric ciphers, namely, stream ciphers and block ciphers.

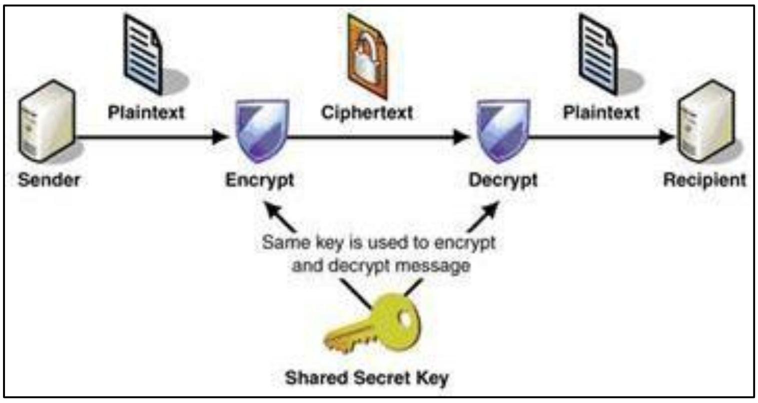
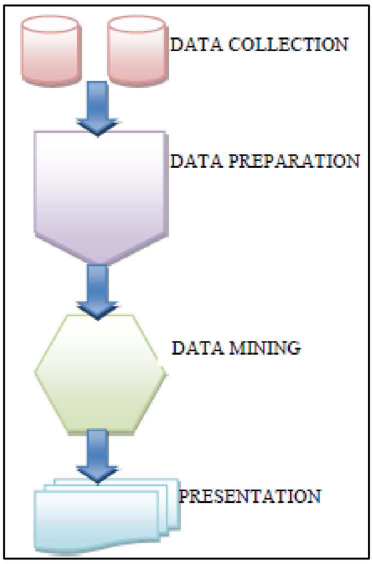


Fig. 4: Symmetric Encryption Technique

VII. DATA MINING MODELS

Data mining is the process of removing useful information or designs from the raw data. Data mining in IoT is used to manage the bulky amount of data which is received from the IoT devices. On the basis of definition of data mining and its functions, a typical data mining process contains these four steps.[14]

1) Data Collection
2) Data preparation
3) Data mining
4) Presentation



Classic data mining models have been separated into four main categories. The first data mining model is the IoT with the Knowledge Discovery Model which plays how the raw data has been transformed into useful information. The second data mining model is the multilayer model in which every layer of the model does their corresponding duties like data collection, data processing and data mining services. The third data mining standard is for distributed architecture which performs and analyses the data stored in the distributed locations. The fourth data mining model is grid founded model which utilizes the extreme amount of data or we may say indefinite data optimally.

Data mining process refers to the process of semi-automatically analyzing huge databases for pattern mining which are innovative, legitimate, useful and understandable which is also known as Knowledge Discovery in Databases (KDD). Data mining or KDD process contains problematic formulation, data collection, data cleaning i.e.

Preprocessing, transformation, choosing mining task/method and result evaluation/visualization. Knowledge discovery is repeated process. This model also contracts with the networking of the data and check data is coming from which environment. Data can be retrieved from database, centralized server and distributed database.

VIII. CHALLENGES

Afar costs and the indistinctness of devices, other security problems plague IoT:

A. Unpredictable Behavior:

The pure volume of organized devices and their long list of enabling technologies means their performance ambiguity the field can be changeable. A specific system may be well planned and within administration control, but there are no assurances about how it will relate with others.

B. Device Similarity:

IoT devices are properly uniform. They utilize the similar connection technology and components. If one system or device suffers from susceptibility, many more have the similar issue.

C. Problematic Deployment

IoT devices are properly uniform. They utilize the similar connection technology and components. If one system or device suffers from susceptibility, many more have the similar issue. Problematic Deployment – One of the core goals of IoT residues to place advanced networks and analytics where they formerly could not go. Unfortunately, this creates the problematic of physically securing the devices in these strange or easily retrieved places.

D. Long Device Life and Expired Support

One of the advantages of IoT devices is longevity, however, that long life also means they may survive their device support. Evaluate this to traditional systems which typically have support and exaltations long after many have stopped using them.

Orphaned devices and abandon ware lack the similar security hardening of other systems due to the progression of technology over time.

E. No Upgrade Support

Several IoT devices, like many mobile phones and small devices, are not planned to allow improvements or any alterations. Others propose inconvenient upgrades, which many owners disregard, or fail to notification.

F. Poor or No Transparency

Several IoT devices fail to deliver transparency with regard to their functionality. Users cannot notice or access their processes, and are left to simulate how devices perform. They have no control over useless functions or data collection; furthermore, when a producer updates the device, it may bring more unwanted functions.

G. No Alerts

Goal of IoT remains to provide its unbelievable functionality without being obvious. This introduces the problem of user consciousness. Users do not observe the devices or know when something goes erroneous. Security breaches can endure over long periods without detection.

IX. CONCLUSION

An IoT device makes a enormous amount of data. To handle data arrival from these devices needs a lot of data management. To produce useful knowledge from the large amount of data we need several data mining techniques. The WSN research community has done an excellent job of addressing some of the limitations that currently exist for healthcare-related functions.

REFERENCES

[1] Gurram [15] Mr. Vishal Kansagara, Mr. Darshan Thoria, Ms. Drashti Hirani,"OVERVIEW ON INTERNET OF THINGS (IoT)"
[2] Petrolo R, Loscrí V, Mitton N. Towards a smart city based on cloud of things. In: Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities - WiMobCity
[3] qusay f. Hassan, "Internet of Things A to Z: Technologies and Applications"
[4] H. Harun and A. Mohd Zin―A Study using Internet of Things Concept toward Engineering Education‖ , Volume 4 No.6, June 2015, Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst03462015.pdf
[5] H. Jiang, X. Chen, S. Zhang, X. Zhang, W. Kong And T. Zhang ―Software for Wearable Devices: Challenges and Opportunities‖ Available Online at http://arxiv.org/ftp/arxiv/papers/1504/1504.00747.pdf
[6] R. John Robles and T. hoon Kim ―Applications, Systems and Methods in Smart Home Technology: A Review‖ Vol. 15, February, 2010 Available Online at www.sersc.org/journals/IJAST/vol15/4.pdf
[7] C. Perera, Member, C.Harold Liu & S.Jayawardena ―The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey‖ Available Online at http://arxiv.org/pdf/1502.00134.pdf
[8] A. Zanella,N. Bui, A. Castellani & L. Vangelista, M.e Zorzi,‖ Internet of Things for Smart Cities‖ IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014
[9] S. Rajguru, S. Kinhekar & S. Pati ― Analysis of Internet of Things in a Smart Environment ―Vol. 4 Issue 4, April-2015, pp: (40-43) Available online at: www.erpublications.com
[10] Air Quality Egg, ―Air Quality Egg,‖ 2013. Retrieved From http://airqualityegg.com/
[11] Amrita Vishwa Vidya Peetham, ―Amritawna: Amrita center for wireless networks and applications,‖ 2013. Retrieved From http://amrita.edu/awna/
[12] D. M. Trivedi1, Prof. T. J. Raval, " Proposed Cryptographic Approach for Securing IOT Device"
[13] Ms. Yogita Pundir, Ms. Nancy Sharma, Dr. Yaduvir Singh, " Internet of Things (IoT) : Challenges and Future Directions"
[14] Divya Joshi, Chanchal Kumari, Abhishek Srivastava, " CHALLENGES AND DATA MINING MODEL FOR IoT"