Journal of Information Technology Management

Print ISSN: 2008-5893
Online ISSN: 2423-5059

IOT Future Security Challenges and Recent Solutions

Khaled Mofawiz Alfawaz*

*Corresponding Author, Department of Management Information System, Faculty of Economics and Administration King Abdulaziz University, Jeddah, Saudi Arabia. E-mail: kalfawaz@kau.edu.sa

Abstract

Internet of Things could be current paradigm, with promising recent wireless communication. Simultaneously as its will likely deliver compelling and effective arrangement, security of the gadgets and organization could be challenge issue. Therefore security has arisen as quite difficult for the IoT during this paper is expect to create security challenges of the IoT, structural design of IoT through handling security troubles at every layer of the design, key advancements in IoT and use of IoT.

Keywords: Internet of Things, Key Technologies, Security Issues

Journal of Information Technology Management, 2022, Vol. 14, No.2, pp. 1-14
Published by University of Tehran, Faculty of Management
doi: https://doi.org/ 10.22059/JITM.2022.86923
Article Type: Research Paper

Received: October 26, 2021
Received in revised form: February 07, 2022
Accepted: March 18, 2022
Published online: April 20, 2022

Introduction

Recently the concept “Internet of Things” has achieved popularity in various domains. It refers to the inter connectivity amongst the daily devices, together with device independence, contextual awareness moreover sensing capability. The devices of Internet of Things include laptops, PCs, tablets, PDAs, smart phones together with hand held embedded devices. Coupled devices furnished various varieties of sensors in addition as actuators observe their surroundings and also recognize the continual performance accordingly. This is often attained through processing the sensed data at a tool hub, node or in an exceedingly. Autonomously the devices are ready to take decisions or propagate data to consumers; through this the users can make the optimal decisions. Interconnected network devices could lead on to a good

number of autonomous still as intelligent applications and services could provide considerable benefits of non-public, professional and economic.

IoT devices create their accessible information to concerned parties such as smart phones, web services as well as cloud resources. Generating this information through the internet is a point, doing this is a controlled direction. Hence, the data objects get connected through the Internet of Things.

According to the recent expansion of internet and its being used in numerous devices with humans, the scope of use of the internet of things is wide broader than it could be visualized. In the year 2020, the authentic IT companies forecasting many devices associated to the internet will exceed 50 billion. This bulky volume of devices linked to the internet refers a much outsized volume data. Hence, considering the nature of this data, which includes with private information like bank account data, medical data etc., it is critical to test the challenges and weaknesses in the security devices and protected the data against potential abusive practices. The software information in internet of things might be corporate, consumable or personal; conversely the stored information should be secure and safe against theft, transport and manipulation. Hence, to elevate the security of Internet of Things, it is mandatory to pay specific attention to the area of storage, method as well as media of transmission, the encryption method, recovery and so on.

Information Technology is revolutionized with the support of Internet of Things that will be utilized in various sectors in the globe to enhance and progress the services with the consumers. IoT defines all kinds devices are connected to the sensor devices through the internet for sending and receiving information. The survey proves that around 20 million devices are to the internet, to stay all the devices, process, people and updating of information along with connecting each other. The IoT will be obtainable in most of the sectors in education, agriculture trends and healthcare.

Iot System Structure

The diverse essence, dynamism, intelligence, mobility additionally undefined perimeters of the IoT make it a popularity innovative area, yet it likewise makes the IoT susceptible and perilous as far as security. The scope of stages on which IoT is open makes it significantly more hard for security specialists to deliver total solutions to the present security concerns. Accordingly, knowing the thought and parts of the IoT becomes critical (Mendez, D. M., et al. 2017)

The establishment for universal computing, whose objective is to attach lifestyle substance to the network utilizing technological stages is made from three parts namely hardware, middleware and presentation respectively. Also, the indistinguishable example can be seen while deciding the standards of th IoT, as per and three variables can be ascribed to the IoT climate, those are,

Based on

- Internet - Things - Semantic

Hence, the identical perception is applied to the IoT organization. The IoT structural design, in step with consists of three layers,

- Perception Layer – PL - Network Layer – NL - Application Layer - AL

The PL collects environmental information, the NL, which comprises of wired as well as remote frameworks, Processes and communicates the information gained through the discernment layer supported by the foundation of innovative The application layer comprises of engrossed explanations that help out the last clients to fulfill their necessities. The IoT needs structural arrangements that can manage heterogeneous states to work expertly and effectively. On the other hand, there is no fused standpoint of the IoT framework. Some designing bodies, including the IEEE and ETSI, have concerned innovation explicit principles including security rules.

Supply Chain Control the executives, Intelligent Shopping Application framework, Smart Product Management framework, Item Tracking framework, Fleet Tracking framework Elegant Shipping Smart handing over via particular greenish blue time on-request visitors statistics and the manner of maximum confined time tour manner improvement.

Applications of Iot

The accompanying table records some of the IoT applications:

Table1: Application of IoT

DOMAIN APPLICATION	EXAMPLES OF APPLICATION
Electronic Health System	Patient Inspecting skeleton, Doctor worldwide positioning framework, Personnel worldwide positioning framework, Real-time affected person wellness repute gazing framework, Predictive mastery statistics to assist professionals along practioner
Trade in addition to Logistics	Supply Chain manage the executives, intellectual Shopping Application framework, Smart Product Management framework, Item pathway framework, Fleet pathway framework
Elegant Shipping	Elegant delivering all the way through unique greenish blue time on-request traffic information and the procedure of most limited time travel way improvement.
Exquisite Situation	Luxurious Homes or Offices, Industrial Plants, Stylish Museum and Gym
Energy Conception	Stylish Peripherals, Stylish Gird
Stylish Residence	Energy utilization, Water utilization, Remote Control,Applications, The arrangement of Intrusion Detection.
Natural Observing	Air Pollution structure, Noise scrutinizing skeleton, Waterways outline, Industry Examing framework.
Green harvest growing	Nourishment, Irrigation executive framework, Soil humidity executive framework.
Futuristic	Robot Cab Management, City Statistics Model Management, Better Game Room Management.

IoT Architecture

In general, the formation of Internet of Things is separated into 4 layers as shown in Fig.1. the common IoT encrusted structural design and its crucial components have been argued below.

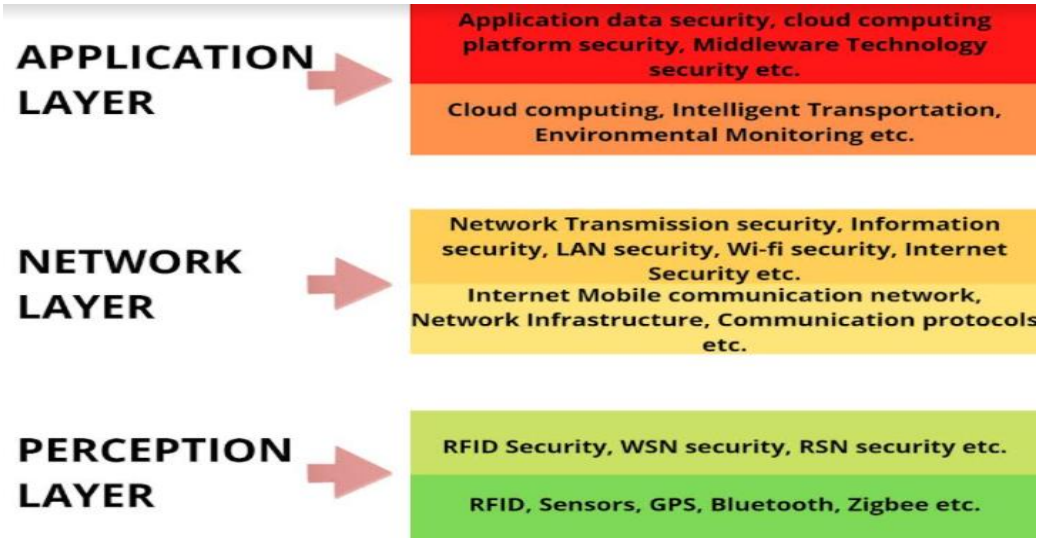

Fig 1. Various Layers with its Applications

A. Perception Layer

The level of perception is likewise referred as the sensing degree. The rule of intelligent sensors works on the availability amongst object, further working with the trade of data amidst them. This layer comprises of joined equipment for perception and obtaining of information (Kumar, S. A., et al. 2016)

1) RFID

RFID has been a essential advancement in the model of surrounded communications, permiting the structure of microchips for wirefree communications. They can be placed in things to permit them to be acknowledged mechanically. RFID labels can be either static or dynamic. static RFID tags do not have interior force, but dynamic RFID tags are self powered and may commence statement.

2) WSN (Wireless Sensor Network)

With modern topical advances in nanotechnology, low power integrated circuits along with tiny gadgets are right now substantially more affordable, offering much superior efficiency and promising low energy expenditure in the concept of remote sensing applications. This has enabled the deployment of a “wireless sensor network” by establishing a slew of intellectual sensor nodes, permiting for collecting data, processing data, analysis data and distribution of appropriate information collected through out the network. The data collected with the assistance of sensors is shared along with them before being transferred for processing, storage as well as analytics (Akyildiz, I. F., et al. 2002).

B. Middleware Layer

This position of middle layer among network along with application layers (AL), for attempting to unintelligible hardware specifics while allowing developers to deliberate on the application implementation procedure. It is in charge of provided that services to customers as well as guaranteeing interoperability, abstraction and scalability. It also substantiate the users to construct a more protected environment as well as proficient service delivery.[5]

1) Data Storage and Analytics

Internet of Things produces enormous amounts of information. As a outcome, the disputes of information storage and analytics become more essential. Presently, the internet consumes approximately five percent of total energy produced internationally and since the Internet of Things is predictable to convey billions of plans throughout the humanity, energy expenditure is bound to rise much higher. As a consequence, it is essential to scrutinize the helpfulness of data centres in order to guarantee intelligent data storage and utilisation for smart monitoring and actuation.

2) Visualization

Visulation is an extra significant viewpoint for an IoT application which incorporates gave that more data to clients through an extra intuitive interface, hence permitting the clients to connect with the adjoining climate. Current headways in the innovation of “touch screen” have advanced the development and method of enhanced tablets and telephones. If the repayment of the IoT upheaval are to show up at the average person, center around amplification of representation that is alluring, effortless to utilize as well as appreciate is essential.

C. Network Layer

The NL gives the simple guide offerings for steady facts switch over the sensor networks. It is likewise answerable for aggregating the records from numerous some types of sources and steerage it to deal with objections. It moves the records over the wi-fi community era like 3G, Wi-fi, Bluetooth, infrared, etc.

1) Data Aggregation

A secured information aggregation method is crucial for making certain the reliable information is being collected from sensor hubs throughout the community (Sang, Y., et al. 2010) As node disappointments are normal in WSNs, the community topology need to be able to recovering itself. Ensuring protection with inside the subject of statistics accumulation may be very important because the community is robotically related to sensors.

2) Addressing Schemes

In IoT, billions of items are imagined to be associated with one another, so it becomes fundamental to manage the cost of interesting recognizable proof for every one of those articles. A tending to plot that solely recognize the articles coordinated across the organization

is a pre-essential to the achievement of IoT (Zorzi, M., et al. 2010).

D. Application layer

This is the crown most layer of the IoT engineering that gives the conveyance of a extensive variety of administrations in specfic fields in IT primary based enterprises like automated, clinical care, instruction, clogistics, groceries production, media simply as environmental checking and so on.

Key Technologies in IoT

Some of the key technologies are considered in IoT like Identification, Sensing and Commnuication Technologies, Middleware, Zigbee Technology and also Cloud Computing.

Identification, sensing and communication technologies

Recognizable proof strategies are electronic items code (EPC) and ubiquitous code (uCode). In IoT, articles' location alludes to the location inside a correspondence network that incorporates IPv6 and IPv4. RFID technology is the fundamental factor in the inserted correspondence technology (Asghar, M. H., et al 2015). It very well may be utilized to screen objects progressively, without the need of being in view. This is useful for planning this present reality into the virtual world. Detecting alludes to gathering of the information from IoT objects inside a similar organization and sending it to the data set or cloud. Items can cooperate with the actual environment either actively or passively performing detecting activities or performing activities.

Middleware

In the Internet of Things, middleware is a network of sub-layers involving the innovation and application levels. It is here and there alluded to as IoT exchange based middleware. Embedded middleware alludes to modules and OS that handle a few communication protocols [9]. It is accountable for offering types of assistance to customers just as ensuring interoperability, adaptability, and reflection. It likewise verifies the client to establish a safer climate just as effective help conveyance.

Cloud computing is the planned consequence of regular PC advancement and association development, for instance, PC innovation and organization innovation, for example, matrix processing, dispersed figuring, equal registering and utility processing, etc. In Internet of Things, there is an immense degree, gigantic proportion of data to be dealt with. So the data dealing with limit is pursued. The data assembled by IoT gadgets are taken care of in the cloud climate. Joined IoT and distributed computing applications enable the creation of brilliant conditions like savvy urban communities, cloud home, etc

Key Layers of Iot

Following are the vital layers for achieving a goal of making IoT.

"Application Layer": Encompasses the various applications and organizations that the IoT gives. Applications join shrewd urban communities, stylish houses, shipping, utilities and clinical benefits.

"Perception Layer": This layer involves various sorts of material advancements, together with heat seansors, sensors of vibration, sensors of pressure and RFID sensors that grant contraptions to recognize various things

"Network Layer": This layer involves association correspondences programming similarly as genuine parts like geologies, servers, network center points, and association parts that license the contraptions to pass on. Its rule object is to convey statistics among devices and from the devices to receivers.

"Physical Layer": The genuine layer includes the principal hardware like real parts, keen devices and power supplies that goes about as spine for frameworks organization the canny article.

Security Issues in "Iot Layers"

With the elevated reception pace of "Internet of Things", an ever increasing number of gadgets are associated with the Web. Consistently, these keen articles are becoming objective for data security chances; IoT can possibly disseminate these dangers definitely more generally than the Web needs to date . The four layers in IoT that need examined before assume the main part in IoT and to formulate IoT dependable and protected.

A. Security Issues in the "Application Layer"

As a result of protection issues in the "application layer", applications can be shut down and compromised with next to no issue. Along these lines, the applications are fail to finish the organizations they are modified to do or even do affirmed organizations incorrectly. Through this layer, toxic attacks can cause errors in the application prograam code that activates the application to breakdown. This is an especially unsafe concern subject to the amounts of contraptions requested as "Application level" components . regular threats to Application Layers are:

Malicious code assaults: A model situation in this sort of assault could be a malignant "worm" spreading on the Web assault installed gadgets running a specific opearting framework gor for example Linux. Could be good for attacking a "extent of little, Web enabled devices" like domastic switches, set crown boxes and observation cameras. The malicious program would use a regarded programming shortcoming to spread. Such code attacks could break into a Vehicle's Wi-Fi. Accept accountability for the controlling wheel, and crash the vehicle achieving wounds to the driver and the vehicle. Hakers exploit application shortcomings on contraption center points and present vindictive root units. The security plan of contraptions ought to be change safe or perhaps adjust obvious. Getting unequivocal bits of a device may be lacking. A couple of risks can handle the nearby

circumstances to make the device mallfuntion aid achieve warming or freezing the atmosphere. A modified temperature sensor might basically display a legitimate worth of hotness, whilst adjusted digital digicam in the sagacious domestic might hand-off old pictures.

B. Security Challenges in the Discernment Layer

The safekeeping risks in the Discernment layer are at center level. Since the centers are contained sensors, they are ideal destinations from software engineers, who want to make use them to update the device programming with their own. In the discernment layer, larger piece of the risks. Ordinary dangers in Insight layer are:

Eves dropping: As the technique for communcation among these gadgets can be remote and through the Web, the gedgets can be vulnerable against eves dropping attacks as the contraptions will all around be left unattended. In this attack circumstance, sensors in the sharp home or m-prosperity region that are compromised can send message spring up to users and undertaking to collect personal information from the customers.

Sniffing Assaults: Assailants can placed malicilous sensors or gadgets near the common sensors of the IoT gadgets, to collect facts from the contraption. The abundance of savvy weather IoT gadgets shows that people may be perceived, traked and orifuked without a doubt all through the real surroundings, without their consent.

C. Security problems in the Network Layer

The organization layer is firmly defenseless against assaults due to the massive quantity of insights that it conveys, this causes a lot of "network clog". Through this layer, the notable security hindrances are with regard to the intergrity and validation of the insights that is being transfered all through the organization. A difficulty commencing programmers along with malevolent hubs that concession gadgets in the organization is a coldblooded concern. Broad dangers has a place with Network layer are:

DoS Assault: The server widgets are overwhelmed with the purpose that they are unable to look at those clients, who require their administrations. DoS arracks that power outage the exchange of information between the gadgets and their assets. A spread out of data is shipped off the gadget that closes down its movement.

Gateway Attacks: Kind of entryway assaults remove relationship among the sensors and the web foundation. This could include DoS assault or steering assaults initiated in the passage that results in incorrect data being sent from the Internet to the sensors.Bottom of Form

Unapproved Access: Gadgets can be left shaky either considering the way that their actual expect that they will continue under their authentic control. Conversely, if they don't, they are available to use by anyone. Implanted miniature gadgets along with full scale contraptions may ought to be left unattended for extensive stretches, in by and large closed off conditions, e.g., pace-creators that are inserted in the human body and distant sensors left in abandoned authentic conditions. These unattended surrounded contraptions, that are utilized for manage, e.g., pacemaker embeds, involve stable wanting to pass on manage signals at set events, after some time are especially perilous for the consumers. As the gadgets will be planned to

converse with various contraptions to send and get data, some dangerous center points may endeavor to veil themselves as checked and also access these devices without having the position and comvinence the devices.

Storage Assaults: Tremendous snippets of information includeing essential data of the customer ought to be taken care of on stockpiles or on cloud, the two of which can be hited and the statistics might be modifed to off base nuances. The replication of the data joined with the passage of data to numerous kinds of community achieves the extended surface area for the attacks.

Injecting False Information: Exterior attackers can mix counterfeit statistics causing the organization to act in response inappropriately or unsafely. This might moreover be a pioneer to a real attack and may be utilized to cover such risks.

D. Security Obstacles in the "Physical Layer"

There are various security concerns at the actual layer of IoT framework also. There is immense requirement for novel innovation to keep up with power sources and considerable security components. Gadgets require to be gotten against actual assaults, commencing people discernment. They additionally want to be power capable and achieved of depending on battery power in the occurrence of a city matrix power outage or energy interfere. Batteries require to get a handle on charge for a satisfactory measure of time and re-energize rapidly to stay the gadget in succession. Normal issues in Physical Layer are:

Physical Damage: Physical devices like sensors, hubs and actuators which might be simply harmed through the pernicious substances. This may want to motive the sensor, hubs and actuators to lose its expected usefulness and turn out to be defenseless to extraordinary dangers.

Environmental Assaults: Sensors which might be assaulted with the herbal obstructions searching like uncommon downpour or snow or wind. This may want to starting the sensor to lose its expected usefulness and defenseless for extraordinary dangers.

Loss of Power: Loss of Power: Devices that ability out of pressure commonly cannot paintings generally and this results in a forswearing of administration. A loss of sleep attack makes without a doubt enough licensed solicitations to live far from a system from getting into its energy-saving mode

Hardware Failure: The devices retain as a lifestyles saver to the patron and it will likely be numerous wards on those devices. In this way, it's far massive that no system disappointments occur which bring about the situation that the system quits operating or a ways extra detestable, starts off evolved sending incorrect figures. Digital attack on terrific city groups could result in a missing inventory of strength or water and bring about confusion.

Physical Altering: In the plant of ground robotization, considerably implanted programmable cause regulators (PLCs) that enact computerized traditions are integrated into the ordinary mission IT framework. It is essential for shield the ones PLCs from human

affiliation and concurrently guard the hobby with inside the IT basis and affect the modern safety controls.

Security Challenges for Iot Enabled Manufacturing

A. Difficulties in Supply Chains

Inventory network is the organization of worries that are in a gathering all the way through upstream just as downstream relationship in a combination of exercises and cycles that form esteem as items and their administrations in the possession of the inevitable client. A distinctive component of smart assembling is that the tasks of assembling are connected to the providers through the web. The labours are associated with supply chains are stream of stock like unrefined components and mindful of conditions.

All individuals inside the related inventory just as creation cycles straightforwardly. For this inspiration IoT works with ongoing seeing of transfer while utilizing a blend of correspondence channels and sensors to create continuous data. Like these true world data will support the produces to diminish stock costs and decide just as decide the issues before they emerge. IoT will approve creators to naturally distinguish the prerequisite to coordinate, refill specifics and items on a machine astute principle, limiting the constraint for the correspondence of individual.

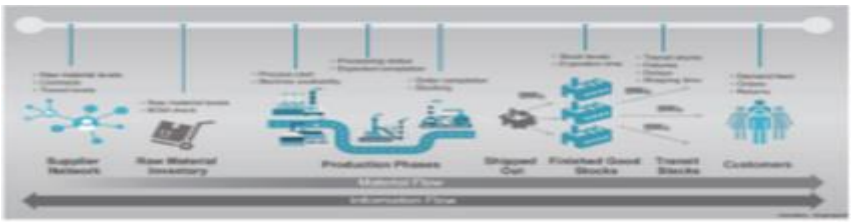

Fig 2. IoT Manufacturing Supply Chains

B. Difficulties in Big Data

It is deliberate that the amount of associated peripherals will enhance to 40 billion via way of means of 2020. An enormous quantity of associated devices simply as sensors will create large degree of data. The large measurements are created thru machines may be requests of length extra noteworthy than that introduced through people in perspective and data introduced via way of means of sensors isn't always in any respect like that produced via way of means of human which is explained in figure 2. Taking care of the potential of Big Data is a test. Continuous response to health evaluation or to catastrophic occasion is essential for data managing and examination.

Relationship of worldly additionally as spatial facts should advise debate in records examination. The uncertainty of the facts is probably sporadic; records recuperation and detail extraction are pivotal elements with inside the influence of records research. The trendy of records research is to create preference for the achievements of machines or people.

Subsequently, high-quality along handy stop posing is an incomprehensible standpoint for records mining. An incredible deal of logical strategies is walking with the facts on a server, desiring in cooperation of pressure and switch velocity to examine the facts to the server. Keen estimation has to be dispersed throughout each the devices and the cloud.

Fig 3. Challenges in Big Data

C. Hardships in Big Data

It is organized that the quantity of associated peripherals will enhance to 40 billion via way of means of 2020. A sizable wide variety of associated gadgets in addition with sensors will make significant percentage of facts. The terrific estimations are made thru machines may be solicitations of length greater vital than that conveyed thru human beings in attitude and information conveyed via way of means of sensors is not in any respect like that brought via way of means of human. Dealing with the restriction of Big Data is a test. Persistent reaction to prosperity assessment or to calamitous event is important for information looking after and evaluation.

Relationship of not unusual place likewise as spatial facts should suggest banter in information evaluation. The vulnerability of the facts can be inconsistent; information healing and thing extraction are vital components with inside the influence of information exam. The norm of information exam is to make selection for the accomplishments of machines or individuals. In this manner, beautiful nearby superb quit providing is a terrific angle for information mining.

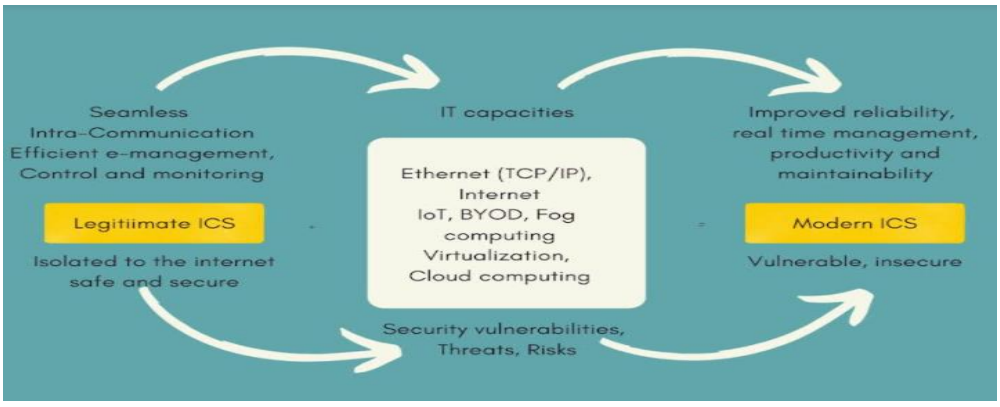

Fig 4. Evolution from legitimate to modern manufacturing systems

Figure 3 portrays the improvement of a valid “Industry Control System” (ICS) to a popular ICS. While a reasonable ICS is coordinated with IT capacities, digital protection concerns are acquainted with the current ICS. As an outcome, digital protection is basic to the achievement of trendy IoT-empowered ICS. The situation is deteriorated by the data that legitimate ICS is for the most part more seasoned gear that isn't suitably ensured against present organized settings. This is because of the way that the parts of a run of the mill ICS communicates utilizing indicated conventions with no security concerns.

A harmful attacker, for instance, may assault a connected computerized car through the remote organization and immediately enter the control framework. The auto business' focus is moving from actual wellbeing of vehicles, drivers and travellers to security assurance alongside digital assaults and interruptions. Accordingly, one most significant issue is deciding how to shield legitimate ICS from attacks while they are associated to the Internet.

D. Challenges in Data Mining

IoT gathers information from many sources, which could possibly encompass required information for IoT. When to utilize information mining to IoT, transforming information procured by IoT into usable data and this data is then changed over into information needed by the client. With the fast paced movement of IoT the basic test is to mining of tremendous information volumes and determines wanted data or information. The central questions of the information mining of IoT are with IoT large information mining need to perform peruse and compose procedure on tremendous measure of information, information stick assembled from various sources and places like from sensors, cameras, trackers, homes, businesses and vehicles and so on (Tretyakov, K. 2004).This data may be in an assortment of organizations and styles, for example, interactive media or text and so on There is association is needed with various sorts of gadgets and various frameworks. As now and again, measurements are significantly obscure and advancement of removing the data is convoluted, suitable investigation on the boundaries of information is required. Different applications include information to be removed and handled continuously examination is needed for different applications to advance information and concentrate information from it. Regardless of whether the informational collections incorporate terabytes or petabytes of the data can be a subject. As the further Technology is IoT empowered computerized reasoning, there are vast methodologies of the Internet of Things and information mining cooperates to build prescient models later on. AI procedures applied on IoT can be utilized concentrate lucky information from colossal volumes of data.

Future Directions

In present day years, IoT has drilled significant improvement in fields like telemedicine stages, canny transportation frameworks, co-ordinations observing and contamination checking frameworks, amidst others. A few analysts expect that the quantity of connected things will arrive at 26 billion constantly of 2020. Then again, the wellbeing inconveniences

associated with IoT should be addressed with the end goal for it to create and develop (He, H., et al. 2016). The ensuing are impending exploration headings for development the Internet of Things safer.

Architecture Standards

IoT as of now uses different gadgets, administrations and conventions to achieve a normal objective. Then again, to consolidate an organization of IoT systems to achieve a greater structure, for instance, to shape a savvy town by the joining of many shrewd homes, there should be a bunch of norms that ought to be followed from the miniature to full scale levels of IoT worry. The current day prerequisite of IoT is to have obvious development norms involving information models, interfaces and conventions that can support a broad assortment of people, gadgets, dialects and working frameworks.

Identity Management

The character the board in IoT is performed by trade recognizing data among the things for first time connection (He, H., et al. 2016) This strategy is helpless to listening in, which can manual for man in-the-center assault and hence can make weak the whole IoT structure. Consequently, there should be some pre-characterized personality the executive element or center point, which can notice the association methodology of gadgets by applying cryptography and different procedures to forestall wholesale fraud.

Conclusion

The diagram of IoT security issues and conceivable outcomes was upheld on an investigation of the larger part ebb and flow research on IoT and Industry. One of the larger part impressive attributes of IoT-empowered brilliant assembling is that collecting procedures are associated to assembling supply chains. There are various shortcomings in the interrelated stock organizations. IoT gadgets will make colossal measures of insights. As the core of knowledge, large information recovery, stockpiling, handling and combination are requesting difficulties. This paper presents the different security issues and difficulties and still there is need for greater security arrangement.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Asghar, M. H., Negi, A., & Mohammadzadeh, N. (2015). Principle application and vision in Internet of Things (IoT). In International Conference on Computing, Communication & Automation (pp. 427-431). IEEE.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016). The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In 2016 IEEE Congress on Evolutionary Computation (CEC) (pp. 1015-1021). IEEE.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS), 5772-5781.

Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879.

Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., & Xiong, N. (2006). Secure data aggregation in wireless sensor networks: A survey. Applications and Technologies, 315-320.

Smart Manufacturing (2005). Iot Enables Fourth Industrial Revolution. Www.Smarttechforyou.Com/2015/03/Smart-Manufacturing-Iot-Fourthindustrial-Revolution.Html,

Tretyakov, K. (2004). Machine learning techniques in spam filtering. In Data Mining Problem-oriented Seminar, MTAT, 3(177), 60-79.

vithya, V. A., Arokiam, L.” A Study Of Security Issues And Challenges In IoT”

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: a wireless-and mobility-related view. IEEE Wireless communications, 17(6), 44-51.

Bibliographic information of this paper for citing:

Alfawaz, Khaled Mofawiz (2022). IOT Future Security Challenges and Recent Solutions. *Journal of Information Technology Management*, 14 (2), 1-14. https://doi.org/ 10.22059/JITM.2022.86923